Preparatory Colloquium
24-27 April 2013, Moscow (Russia)
Section II: Information Society and Penal Law

JAPAN*

Kanako TAKAYAMA / Chu-wen ZHAO*

I Legislative Practices and Legal Concepts

(a) Criminal laws related to cybercrimes in Japan

The present Penal Code of Japan (1907) has only about three hundred provisions that basically define traditional crimes such as murder and theft. Although some cybercrimes have been introduced into the Penal Code, many offenses are defined in several so-called special criminal laws such as the Telecommunications Services Act, the Wire Telecommunications Act, the Wireless Telegraphy Act, the Act on Prohibition of Unauthorized Computer Access, and so on.

1. Penal Code[1] (Act No. 45 of 1907)

Offenses in the Penal Code are the following:

Chapter XVII Crimes of Counterfeiting of Documents

Article 157 (False Entries in the Original of Notarized Deeds)[2]

(1) A person who makes a false statement before a public officer and thereby causes the official to make a false entry in the original of a notarized deed, such as the registry or family registry, relating to rights or duties, or to create a false record on the ***electromagnetic record***[3] *to be used as the original of a notarized deed relating to rights or duties shall be punished by imprisonment with labor for not more than five years or a fine of not more than*

---

* Important notice: this text is the last original version of the national report sent by the author. The Review has not assured any editorial revision of it.

* Kanako TAKAYAMA, Professor of Law, Kyoto University / Chu-wen ZHAO, Research Assistant at the Faculty of Law, Kyoto University.

1 An English translation of some laws is available on the website of the government: http://www.japaneselawtranslation.go.jp/?re=02.

2 Articles 7-2, 157-2, 158, 161-2, 234-2, 246-2, 258, and 259 were either introduced or changed in the amendment of the Penal Code in 1987.

3 The bold face in the text is given by national reporters. As for the definition of "electromagnetic record," see *infra* **II (a) 2a**.

500,000 yen.

(3) An attempt[4] of the crimes proscribed under the preceding two paragraphs shall be punished.

Article 158 (Uttering of Counterfeit Official Documents)

(1) A person who utters a document or drawing proscribed in the preceding four articles or provides the ***electromagnetic record*** *proscribed in Paragraph (1) of the preceding article for use as the original of a notarized deed shall be punished by the same penalty as a person who counterfeits or alters a document or drawing, makes a false document or drawing, or causes a false entry or record to be made.*

(2) An attempt of the crimes proscribed under the preceding paragraph shall be punished.

Article 161-2 (Unauthorized Creation of Electromagnetic Records)

(1) A person who, with the intent to bring about improper administration of the matters of another person, unlawfully creates without due authorization an ***electromagnetic record*** *which is for use in such improper administration and is related to rights, duties, or certification of facts shall be punished by imprisonment with labor for not more than five years or a fine of not more than 500,000 yen.*

(2) When the crime proscribed under the preceding paragraph is committed in relation to an ***electromagnetic record*** *to be created by a public office or a public officer, the offender shall be punished by imprisonment with labor for not more than ten years or a fine of not more than 1,000,000 yen.*

(3) A person who, with the intent proscribed in Paragraph (1), puts an ***electromagnetic record*** *created without due authorization and is related to rights, duties, or certification of facts into use for the administration of the matters of another shall be punished by the same penalty as the person who created such an electromagnetic record.*

(4) An attempt of the crime proscribed under the preceding paragraph shall be punished.

Chapter XVIII-2 Crimes Related to Electromagnetic Records of Payment Cards

[4] The penalty for attempts can be reduced according to Articles 44 and 68. Usually, the maximum and minimum terms of imprisonment become half of each.

Article 163-2 (Unauthorized Creation of Electromagnetic Records of Payment Cards)[5]

(1) A person who, for the purpose of bringing about improper administration of the financial affairs of another person, creates without due authorization an ***electromagnetic record*** *which is for use in such improper administration and is encoded in a credit card or other cards for the payment of charges for goods or services shall be punished by imprisonment for not more than ten years or a fine of not more than 1,000,000 yen. The same shall apply to a person who creates without due authorization an* ***electromagnetic record*** *which is encoded in a card for withdrawal of money.*

(2) A person who, for the purpose proscribed in the preceding paragraph, puts an unlawfully created ***electromagnetic record*** *proscribed in the same paragraph into use for the administration of the financial affairs of another person shall be dealt with in the same way as prescribed in the same paragraph.*

(3) A person who, for the purpose proscribed in Paragraph (1), transfers, lends, or imports a card encoded with an unlawful ***electromagnetic record*** *proscribed in the same paragraph shall be dealt with in the same way as prescribed in the same paragraph.*

Article 163-3 (Possession of Payment Cards with Unauthorized Electromagnetic Records)

A person who, for the purpose proscribed in Paragraph (1) of the preceding article, possesses the card proscribed in Paragraph (3) of the same article shall be punished by imprisonment with labor for not more than five years or a fine of not more than 500,000 yen.

Article 163-4 (Preparation for Unauthorized Creation of Electromagnetic Records of Payment Cards)

(1) A person who, for the purpose of use in the commission of a criminal act proscribed in Paragraph (1) of Article 163-2, obtains information for the ***electromagnetic record*** *proscribed in the same paragraph shall be punished by imprisonment with labor for not more than three years or a fine of not more than 500,000 yen. The same shall apply to a person who, knowing the purpose of the obtainer, provides the information.*

---

[5] Articles from 163-2 to 163-5 were introduced by the amendment in 2001.

(2) A person who, for the purpose proscribed in the preceding paragraph, stores the illegally obtained information of an ***electromagnetic record*** *proscribed in Paragraph (1) of Article 163-2 shall be dealt with in the same way as prescribed in the preceding paragraph.*

(3) A person who, for the purpose proscribed in Paragraph (1), prepares instruments or materials shall be dealt with in the same way as prescribed in the same paragraph.

Article 163-5 (Attempts)

An attempt of the crimes proscribed under Article 163-2 and Paragraph (1) of the preceding article shall be punished.

Chapter XXI-2 Crimes Related to Electromagnetic Records to Give Unauthorized Commands[6]

Article 168-2 (Use of Electromagnetic Records to Give Unauthorized Commands, etc.)

(1) A person who, for the purpose of using the computer of another, creates or offers one of the following electromagnetic or other records without justifiable grounds shall be punished by imprisonment with labor of not more than three years or a fine of not more than 500,000 yen.

(i) An electromagnetic record that gives unauthorized commands to interfere with the operation of a computer utilized by another or to cause such a computer to operate counter to the purpose of such utilization, or to obstruct the business of another by interfering with the operation of a computer utilized for the business of another or by causing such computer to operate counter to the purpose of such utilization by damaging such computer or any electromagnetic record used by such computer, by inputting false data, or by giving unauthorized commands

(ii) An electromagnetic or other record except that proscribed in Item (i) that gives the unauthorized commands proscribed in Item (i)

(2) The same shall apply to anyone who uses an electromagnetic record proscribed in Item (i) of the preceding paragraph for the purpose of execution in a computer of another without justifiable grounds.

---

[6] Articles 168-2, 168-3, and 234-2 (2) were introduced by the amendment in 2011 and are therefore not included in the English translation dated April 1, 2009.

(3) An attempt to commit the crime proscribed under the preceding paragraph shall be punished.

Article 168-3 (Obtaining Electromagnetic Records to Give Unauthorized Commands, etc.)

A person who, for the purpose proscribed in Paragraph (1) of Article 168-2, obtains or stores without justifiable grounds an electromagnetic record proscribed in the same paragraph shall be punished by imprisonment with work for not more than two years or a fine of not more than 300,000 yen.

Chapter XXXV Crimes against Credit and Business

Article 234-2 (Obstruction of Business by Damaging a Computer)

(1) A person who obstructs the business of another by interfering with the operation of a ***computer*** *utilized for the business of the other or by causing such* ***computer*** *to operate counter to the purpose of such utilization by damaging such* ***computer*** *or any* ***electromagnetic record*** *used by such* ***computer****, by inputting false data or giving unauthorized commands, or by any other means, shall be punished by imprisonment with labor for not more than five years or a fine of not more than 1,000,000 yen.*

(2) An attempt of the crime proscribed under the preceding paragraph shall be punished.

Chapter XIII Crimes of Violating Confidentiality

Article 246-2 (Computer Fraud)

In addition to the provisions of Article 246[7]*, a person who obtains or causes another to obtain profit by creating a false* ***electromagnetic record*** *relating to acquisition, loss, or alteration of property rights by inputting false data or giving unauthorized commands to a* ***computer*** *utilized for the business of another, or by putting a false* ***electromagnetic record*** *relating to acquisition, loss, or alteration of property rights into use for the administration of the matters of another shall be punished by imprisonment with labor for not more than ten years.*

Chapter XL Crimes of Destruction and Concealment

Article 258 (Damaging of Documents for Government Use)

A person who damages a document or an ***electromagnetic record*** *in use by a public office shall be*

[7] Traditional fraud directed to natural persons.

punished by imprisonment with labor for not less than three months but not more than seven years.

Article 259 (Damaging of Documents for Private Use)

A person who damages a document or ***electromagnetic record*** *of another that concerns rights or duties shall be punished by imprisonment with labor for not more than five years.*

2. Act on Prohibition of Unauthorized Computer Access (Act No. 128 of 1999)[8]

Article 3 (Prohibition of Unauthorized Access)

No person shall have ***unauthorized computer access*** [to a limited-use network[9]].

Article 11 (Penal Provision)

A person who has violated the provisions of Article 3 shall be punished by imprisonment with labor for not more than three years or a fine of not more than 1,000,000 yen.

Articles 4-7 *(Prohibition of obtaining, offering, storing, and "phishing" identification codes of another for the purpose of unauthorized access) and* ***Article 12*** *(Punishment of those conducts by imprisonment with labor for not more than one year or a fine of not more than 500,000 yen)*

3. Telecommunications Services Act (Act No. 86 of 1984)

Article 179 *(Punishment of infringement of secrecy[10] of telecommunications services by imprisonment with labor for not more than two years or a fine of not more than 1,000,000 yen, aggravated to three years and 2,000,000 yen if committed by a personnel member; attempts punishable in both cases)*

Article 190 *(Punishment of legal entities by increased fines)*

4. Wire Telecommunications Act (Act No. 96 of 1953)

Article 9 *(Prohibition of infringement of secrecy of wire telecommunications services other than in the*

[8] An English translation of the version before the amendment is available on the website of the National Police Agency: http://www.npa.go.jp/cyber/english/legislation/ucalaw.html.
[9] Complemented by national reporters.
[10] Article 21 Paragraph 2 of the Constitution stipulates as follows: "No censorship shall be maintained, nor shall the secrecy of any means of communication be violated."

aforementioned act)

Article 14 *(Punishment of conduct against Article 9 by imprisonment with labor for not more than two years or a fine of not more than 500,000 yen, aggravated to three years and 1,000,000 yen if committed by a personnel member; attempts punishable in both cases)*

Article 18 *(Punishment of legal entities by increased fines)*

5. Radio Law (Act No. 131 of 1950)

Article 106 *(1) (Punishment of distributing false information by means of wireless telecommunications services for the purpose of promoting one's own interest or inflicting damage on another by imprisonment with labor for not more than three years or a fine of not more than 1,500,000 yen)*

Article 107 *(Punishment of instigation of an insurrection by means of wireless telecommunications services by imprisonment with or without labor for not more than five years)*

Articles 108 *(Punishment of distributing obscene information by means of wireless telecommunications services by imprisonment with labor for not more than two years or a fine of not more than 1,000,000 yen)*

6. Act on Punishment of Activities Relating to Child Prostitution and Child Pornography, and the Protection of Children (Act No. 106 of 2004)

Article 7 *(Provision of Child Pornography and Other Related Activities)*[11]

(1) Any person who provides child pornography shall be sentenced to imprisonment with work for not more than three years or a fine of not more than 3,000,000 yen. The same shall apply to a person who provides ***electromagnetic records*** *or any other record which depicts the pose of a child which falls under any of the items of Paragraph 3 of Article 2* [definition of child pornography]*, in a visible way* ***through electric telecommunication lines****.*

(2) Any person who produces, possesses, transports, imports to, or exports from Japan child

[11] In Japanese law, a "child" means a person who is eighteen years old or younger. A "minor" means a person who is nineteen years old or younger.

pornography for the purpose of the activities proscribed in the preceding paragraph shall be punished by the same penalty as is prescribed in the said paragraph. The same shall apply to a person who retains the ***electromagnetic records*** *proscribed in the preceding paragraph for the purpose of the same activities.*

(4) Any person who provides child pornography to unspecified persons or a number of persons, or displays it in public, shall be sentenced to imprisonment with work for not more than five years and/or a fine of not more than 5,000,000 yen. The same shall apply to a person who provides ***electromagnetic records*** *or any other record which depicts the pose of a child which falls under any of the items of Paragraph 3 of Article 2 to unspecified persons or a number of persons in a visible way* ***through telecommunication lines****.*

(5) Any person who produces, possesses, transports, imports to, or exports from Japan child pornography for the purpose of the activities proscribed in the preceding paragraph shall be punished by the same penalty as is prescribed in the said paragraph. The same shall apply to a person who retains the ***electromagnetic records*** *proscribed in the preceding paragraph for the purpose of the same activities.*

Article 11 *(Punishment of legal entities)*

Among these special laws, the Act on Prohibition of Unauthorized Computer Access and the Act on Punishment of Activities Relating to Child Prostitution and Child Pornography, and the Protection of Children were made in response to international circumstances rather than because of internal problems. In 1999, all G7 (Group of Seven) developed countries except Japan had already criminalized this conduct. Punishment of child pornography was introduced in order to ratify the Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography of 2000. The introduction of Chapter XVIII-2 Crimes Related to Electromagnetic Records of Payment Cards into the Penal Code in 2001 was also influenced by the G8's Lyon Group against international crime.

The most recent amendments of the Penal Code introduced new offenses relating to so-called computer viruses. The Act on Prohibition of Unauthorized Computer Access, after its amendment in 2012, punishes the obtaining of an identification code of another person with regard to a technological restriction measure (Article 2 (2)) for the purpose of unauthorized access (Article 4) and storage of such an illegally obtained code for the same purpose (Article 6).

(b) Impact of judicial decisions on the formulation of criminal law[12]

Until recently, Japanese legislators were not very active in making new criminal provisions or amending existing laws. The judicative instead played a role of the Diet through extended interpretation of criminal laws, although it did not have the authority to make laws.

For example, the Supreme Court declared in its decision in 1983 that electromagnetic records fell under "the original of a notarized deed" in Article 157 before its amendment.[13] However, since "the original of a notarized deed" was regarded as a kind of "document" (on paper), scholars strongly criticized the decision, as it violated the principle of legality (*nulla poena sine lege*). In 1987, the Penal Code was amended to include "electromagnetic records" in the provisions mentioned above in **(a)**. Even after that, the Supreme Court newly applied Article 162 of the Penal Code for punishment of delivery of altered securities to selling electromagnetic phone cards for telephone booths, although securities were supposed to be documents as well.[14] The Penal Code has not been amended after this dubious decision while it has been followed by legal practice as case law.

A similar undesirable effect was the result of the Supreme Court's decision in 2001. Article 175 of the Penal Code was as follows until 2011:

> ***Article 175 (Distribution of Obscene Objects)*** before amendment
>
> *A person who* ***distributes, sells, or displays in public an obscene document, drawing, or other object*** *shall be punished by imprisonment with work for not more than two years, a fine of not more than 2,500,000 yen, or a petty fine. The same shall apply to a person who possesses the same for the purpose of sale.*

The accused in the case offered electromagnetic data of sexually explicit pictures to several persons through the Internet. The Penal Code defined "electromagnetic data" as intangible (Article 7-2). Since the data did not fall under "document, drawing, or other object," punishment of "distribution" did not apply, either. The Court strangely declared the conduct to be "display in public" of an obscene "object," by ruling that the "obscene object" in this case meant a

---

12 The website of the Supreme Court offers some English translations of its important judgments: http://www.courts.go.jp/english/

13 Decision on November 24, 1983, Supreme Court Reporter in Criminal Matters (*Keishu*) Vol. 37, No. 9, p. 1538 ff.

14 Decision on April 5, 1991, Supreme Court Reporter in Criminal Matters (*Keishu*) Vol. 45, No. 4, p. 171 ff.

hard disk of a host computer storing electromagnetic data of an obscene graphic image.[15] It was against the common understanding of "display" because none of his clients was able to see the computer.

The legislator in 2011 left the decision untouched. The amendment of the Penal Code in 2011 criminalized "possession" of electromagnetic data storage media and "storage" of electromagnetic records with regard to pornography (Article 175 of the Penal Code). The new provision still targets only tangible objects with regard to "display," while it is questionable whether a "data storage medium" can be displayed. Obviously, distribution of electromagnetic data as such has been included in the new second sentence of the first paragraph.

Article 175 (Distribution of Obscene Objects) since 2011

(1) A person who distributes or ***displays in public*** *an obscene document, drawing,* ***data storage medium of electromagnetic records,*** *or other* ***object*** *shall be punished by imprisonment with work for not more than two years, a fine of not more than 2,500,000 yen, or a petty fine, or by imprisonment and a fine. The same shall apply to a person who distributes obscene electromagnetic records through a telecommunications line.*

(2) The same shall apply to a person who, for the purpose of sale, possesses the objects proscribed in the preceding paragraph or stores the electromagnetic records proscribed in the preceding paragraph.

Although there is now more criminal legislation than before, its response to social change tends to be slower than that of case law.

(c) Legislative Techniques

Since amendments of criminal laws are not frequent, cybercrime laws have not yet been unified into one law. The technique of recasting is being used in the field of traffic accident offenses that were previously scattered in different provisions in the Penal Code and in the Road Traffic Act.

In Japanese law, it is often the case that laws made by the Diet delegate administrative organs to regulate the details of their contents. It is called "delegated legislation" and is particularly used in the field of illegal drug control. The

[15] Decision on July 16, 2001, Supreme Court Reporter in Criminal Matters (*Keishu*) Vol. 55, No. 5, p. 317 ff. An English translation is available on the website of the Supreme Court: http://www.courts.go.jp/english/judgments/text/2001.07.16-1999.-A-.No..1221.html.

basic law contains only general notions of offenses and penalties. Details are given by delegated administrative organs in the form of regulations or orders. It enables social changes to be caught up with but is not used for cybercrimes in Japan.

II Specific Cybercrime Offenses

Concerning *mens rea*, cybercrime offenses must be intentional (at least with *dolus eventualis*). There are no negligent offenses in this field.

Many offenses require a specific intent in the form "for the purpose of," as in the Penal Code. This purpose is supposed to mean a future danger of violation of interests of another or society, while *actus reus* as such still remains in the phase of preparation. For example, Possession of Payment Cards with Unauthorized Electromagnetic Records (Article 163-3 of the Penal Code) as such does not harm another. However, if the person has a "purpose of bringing about improper administration of the financial affairs of another person," then there is certain danger of future harm.

The exception to such purposes can be seen in Article 106 of the Radio Law (above). "The purpose of promoting one's own interest or inflicting damage on another" does not increase the danger of false information. This purpose is regarded as an element that aggravates the blameworthiness of the actor.

There are some offenses in which the burden of proof is switched with regard to the knowledge of the accused. One example is the Act on Punishment of Activities Relating to Child Prostitution and Child Pornography, and the Protection of Children (above).

Article 9 *(Knowledge of the Age of the Child)*

No one who uses a child shall be exempt from punishment pursuant to the provisions of Articles 5 to 8 on the grounds of lacking knowledge of the age of the child. However, this shall not apply in cases where there is no negligence.

(a) Integrity and functionality of the IT system

1. Illegal access and interception of transmission

a. Object – system or data?

Japanese criminal laws punish both attack against a computer system and that against data. For example, Article 234-2 of the Penal Code (above) punishes both the obstruction of business by damaging a computer and that by inputting false data or giving unauthorized commands. Physical attack against telecommunications services is also punishable under the Telecommunications Services Act and the Wire Telecommunications Act.

Deleting electromagnetic records is punished as Damaging of an Electromagnetic Record under Articles 258 and 259 of the Penal Code. Offenses relating to computer viruses have been criminalized under Articles 168-2 and 168-3 of the Penal Code (above).

b. Requirement of infringement of security measures?

Article 2 (4) of the Act on Prohibition of Unauthorized Computer Access requires as an element of the offense of "unauthorized access" at least one of the following conditions:

(i) unauthorized input of an identification code into a computer for restricted use

(ii) unauthorized input of another command into a computer that enables escape from its security measures

(iii) unauthorized input of such a code or command into a computer through another computer connected by a network

2. Data and system interference

a. Object – protection of system/hardware/data?

Although the Penal Code does not define "computer," it gives a definition of "electromagnetic record" since the amendment of 1987.

> ***Article 7-2*** *(Definition)*
>
> *The term "electromagnetic record" as used in this Code shall mean any record that is produced by*

electronic, magnetic, or any other means unrecognizable by natural perceptive functions and is used for data-processing by a computer.

b. Act – destruction/alteration/rendering inaccessible?

The Penal Code penalizes unauthorized production and alteration in Articles 157 and 161-2 (above). Unauthorized erasure is also a criminal offense under Articles 258 and 259 (above).

The Telecommunications Services Act, the Wire Telecommunications Act, and the Radio Law punish the unauthorized interception of the transmission of electronic information.

3. Data Forgery

a. Object – authenticity?

Does your penal law define as a criminal offense the unauthorized input, alteration, deletion, or suppression of computer or electronic data resulting in inauthentic data in order to protect the authenticity of the data to be used or acted upon for legal purposes? If you have a definition, please provide it along with reference to the related paragraphs/articles of your code and/or special statutes.

The Penal Code distinguishes between the creation of false information on the one hand (Articles 156 and 160) and the creation of false authenticity on the other hand (Articles 155 and 159) very clearly in offenses of document forgery. However, authenticity is not always evident in the case of electromagnetic records. Therefore, the legislator decided not to make two different provisions for this and introduced only Articles 161-2 (above) to punish both cases.

b. Act – alteration/deletion?

Does your penal law penalize as a criminal offense the unauthorized input, alteration, deletion, or suppression of computer or electronic data/information resulting in inauthentic data/information with the intent that it be considered or acted upon for legal purposes as if it were authentic? If yes, please provide reference to the applicable paragraphs/articles of your code.

Since the offense in Article 161-2 of the Penal Code does not require that the data created pretend authenticity, as mentioned in **a**, Article 157 is the only provision that makes it a condition of the offense that the altered record is still

to be used "as the original of a notarized deed relating to rights or duties."

4. Misuse of Devices

a. Object – type of device?

Although Japanese law did not criminalize preparation of hacking for a long time, the amendment of the Penal Code in 2011 introduced offenses of developing, obtaining, and storing of electromagnetic records to give unauthorized commands (Articles 168-2 and 168-3, above), which included punishment of preparation for unauthorized access. In the same year, preparation of identification codes for unauthorized access also became punishable under the Act on Prohibition of Unauthorized Computer Access (Article 12, above).

b. Act – public distribution/transfer to another person?

The Act on Prohibition of Unauthorized Computer Access does not penalize an attempt of unauthorized access. However, Article 168-2 Paragraph (2) of the Penal Code (above) explicitly criminalizes the "use" of an electromagnetic record that gives an unauthorized command for the purpose of execution in a computer of another without justifiable grounds. Even an attempt is punishable in (3).

The public distribution and/or transfer to other parties of hacked electronic information is not punishable in the Penal Code but can constitute a criminal offense if it falls under the Telecommunications Services Act or the Wireless Telecommunications Act (above).

c. Possession?

By the amendment of the Penal Code in 2001, the mere possession of a hacker's "tool kit" was criminalized "for the purpose of using the computer of another to create or offer one of the following electromagnetic or other records without justifiable grounds" (Article 168-3, above).

(b) Privacy

1. Violation of Secrecy of Private Data

a. Object – type of private data?

Japan recently introduced special laws to regulate the collecting of private information. The Act on the Protection of

Personal Information (Act No. 119 of 2003) requires data collectors to disclose their information practices in the following provisions:

Article 16 *(Restriction by the Purpose of Utilization)*

(1) A business operator handling personal information shall not handle personal information about a person, without obtaining the prior consent of the person, beyond the scope necessary for the achievement of the Purpose of Utilization specified pursuant to the provision of the preceding article.

Article 17*(Proper Acquisition)*

A business operator handling personal information shall not acquire personal information by deception or other wrongful means.

Article 18 *(Notice of the Purpose of Utilization at the Time of Acquisition, etc.)*

(1) When having acquired personal information, a business operator handling personal information shall, except in cases in which the Purpose of Utilization has already been publicly announced, promptly notify the person of the Purpose of Utilization or publicly announce the Purpose of Utilization.

Article 25 *(Disclosure)*

(1) When a business operator handling personal information is requested by a person to disclose such retained personal data as may lead to the identification of the person (such disclosure includes notifying the person that the business operator has no such retained personal data as may lead to the identification of the person concerned; the same shall apply hereinafter), the business operator shall disclose the retained personal data without delay by a method prescribed by a Cabinet Order. However, when falling under any of the following items, the business operator may keep all or part of the retained personal data undisclosed:

……

Article 34 *(Recommendations and Orders)*

(1) When a business operator handling personal information has violated any of the provisions of Article 16 to Article 18, Article 20 to Article 27, or Paragraph (2) of Article 30, a competent Minister may recommend that the

business operator handling personal information cease the violation and take other necessary measures to correct the violation when the competent Minister finds it necessary for protecting the rights and interests of individuals.

***Article 56** (Punishment)*

A business operator who violates orders issued under Paragraph (2) or (3) of Article 34 shall be sentenced to imprisonment with work of not more than six months or to a fine of not more than 300,000 yen.

In the field of electronic commerce, there is stronger protection of consumers:

***Article 18** (Notice of the Purpose of Utilization at the Time of Acquisition, etc.)*

*(2) Notwithstanding the provision of the preceding paragraph, when a business operator handling personal information acquires such personal information on a person as is written in a contract or other document (including a record made by **an electronic method**, a magnetic method, or any other method not recognizable to the human senses; hereinafter, the same shall apply in this paragraph) as a result of **concluding a contract** with the person or acquires such personal information on a person as is written in a document directly from the person, the business operator shall **expressly show** the Purpose of Utilization **in advance**.*

This is combined with the duties of a business operator prescribed in the Act on Specified Commercial Transactions (Act No. 57 of 1976) that obliges mail-order sales providers to indicate certain information on "terms and conditions" beforehand (Article 12).

The Act on the Protection of Personal Information Held by Administrative Organs (Act No. 58 of 2003) also requires a clear indication of the purpose of use (Article 4), disclosure (Article 12), and so on, although the act or omission by the state is not punishable.

b. Act – illegal use and transfer/distribution?

The Act on the Protection of Personal Information mentioned above in **a** does not penalize the transfer and distribution of private data as such (punishment is possible only under Article 56). However, if the data fall under "trade secrets," such conducts are very widely punishable by the Unfair Competition Prevention Act (Act No. 47 of 1993). Its Article 21 penalizes unauthorized acquisition, use, disclosure, reproduction, storage, and so on.

c. Justification?

General justification such as self-defense, necessity, and exercise of constitutional rights applies to all criminal offenses. Besides, it is important that the Act on the Protection of Personal Information justify transfer of personal data only under such strict conditions as for example its Article 16 shows:

> ***Article 16*** *(Restriction by the Purpose of Utilization)*
>
> *(3) The provisions of the preceding two paragraphs shall not apply to the following cases:*
>
> *(i) Cases in which the handling of personal information is based on laws and regulations*
>
> *(ii) Cases in which the handling of personal information is necessary for the protection of the life, body, or property of an individual and in which it is difficult to obtain the consent of the person*
>
> *(iii) Cases in which the handling of personal information is specially necessary for improving public health or promoting the sound growth of children and in which it is difficult to obtain the consent of the person*
>
> *(iv) Cases in which the handling of personal information is necessary for cooperating with a state organ, a local government, or an individual or a business operator entrusted by either of the former two in executing the affairs prescribed by laws and regulations and in which obtaining the consent of the person is likely to impede the execution of the affairs concerned*

Other articles in the Act and also the Act on the Protection of Personal Information Held by Administrative Organs require similar conditions.

2. Violation of professional confidentiality

a. Object – type of private data?

Japanese law in general does not require that professionals such as medical doctors, dentists, pharmacists, attorneys, persons with religious occupation, and so on disclose their information policies. However, one example is as follows:

> ***Article 134*** *(Unlawful Disclosure of Confidential Information)*
>
> *(1) When a physician, pharmacist, pharmaceuticals distributor, midwife, attorney, defense counsel, notary*

public, or any other person formerly engaged in such profession discloses, without justifiable grounds, another person's confidential information which has come to be known in the course of such profession, imprisonment with work for not more than six months or a fine of not more than 100,000 yen shall be imposed.

(2) The same shall apply to cases where a person who is or was engaged in a religious occupation discloses, without justifiable grounds, another person's confidential information which has come to be known in the course of such religious activities.

Similar penal provisions are included in all the laws regulating professions that require a special qualification such as in the Act on Public Health Nurses, Midwives, and Nurses (Act No. 203 of 1948). In addition, the National Public Service Act (Act No. 120 of 1947) and the Local Public Service Act (Act No. 261 of 1950) penalize unauthorized disclosure of secret information obtained in the course of public functions. Since "confidential information" and "secret" are not restricted in their content, the scope of these offenses can be considerably wide.

Justification applies to these offenses as well according to the principles mentioned above in **1 c**.

b. Subject – type of perpetrator?

As mentioned above in **a**, all professionals whose qualification is regulated by law and all public officials including parliament members, judges, and prosecutors stand under the penal provisions to punish violation of personal secrets. In the case of trade secrets, a person who makes a contract in that regard can be punished by the Unfair Competition Prevention Act as stated in **1 b**.

c. Act – illegal use and transfer/distribution?

Which acts (e.g., illegal collection, use, transfer, and distribution) are specifically penalized by your country's criminal law?

Collection of personal data is not a criminal offense as such unless it violates special protections as in the Telecommunications Services Act, the Wire Telecommunications Act, the Unfair Competition Prevention Act, and the Act on Prohibition of Unauthorized Computer Access.

Use, transfer, and distribution of such data can be punished by the laws mentioned above in **1** and **2 a**.

3. Illegal processing of personal and private data

a. Object?

Illegal acquisition of personal data constitutes a crime in the case of identification codes in the Act on Prohibition of Unauthorized Computer Access (Article 7, above) and in the case of personal information in the Act on Protection of Personal Information (Article 17, above). Acquisition, storage, and transfer of credit card and other payment card information are punishable according to Article 163-4 of the Penal Code (above). Use of such information falls under Article 163-2 (2).

Contrary to the case of personal data, unauthorized conducts relating to private data have not been widely criminalized. The only exception seems to be data-processing of trade secrets in the sense of the Unfair Competition Prevention Act as mentioned above in **1 b**.

Manipulation of electromagnetic data is in general punishable by Article 161 (1) of the Penal Code if the conduct was with the intent to bring about improper administration of the matters of another person.

b. Subject?

The categories of persons under the obligation to protect personal secrets are defined in the Penal Code (Article 134) and each special law that gives qualification to professionals (**2 a**). Public officials are defined in the National Public Service Act, the Local Public Service Act, and other related special laws.

Article 2 (3) of The Act on Protection of Personal Information defines the term “a business operator handling personal information” as “a business operator using a personal information database, etc. for its business.”

Legal entities can be punished for the offenses in the Telecommunications Services Act, the Wireless Telecommunications Act, the Act on Punishment of Activities Relating to Child Prostitution and Child Pornography, and the Protection of Children, the Unfair Competition Prevention Act, and the Act on Protection of Personal Information.

c. Act?

Collection and retention of personal and private data have not been generally criminalized as mentioned above in **a**.

Illegal use can be widely punished in the case of trade secrets. Illegal transfer of personal and private data is also widely punishable if the information is a personal secret as mentioned above in **2 a**.

Use and transfer of these personal and private data are permitted for police or law enforcement purposes as prescribed in, for example, Article 16 (3) (iv) of the Act on Protection of Personal Information as in "cases in which the handling of personal information is necessary for cooperating with **a state organ**, **a local government**, or an individual or a business operator entrusted by either of the former two in executing the affairs prescribed by laws and regulations and in which obtaining the consent of the person is likely to impede the execution of the affairs concerned."

d. Justification?

Since the Constitution guarantees the freedom to choose occupation (Article 22), there may not be a general restriction on the collection, processing, and use of information. Still, the article makes it a condition for such freedom in "that it does not interfere with public welfare."

The Act on Protection of Personal Information also mentions the "usefulness of personal information" in its Article 1.

Thus, since Japanese law does not generally prohibit processing of personal and private data, "justification" does not come into question. Only if the conduct interferes with public welfare may the State restrict or punish it as in cases of violation of personal or trade secrets, defamation, instigating crimes, data forgery, disturbance of business, and so on.

4. Identity theft

a. Object

So-called "phishing" has recently been penalized by the amendment of the Act on Prohibition of Unauthorized Computer Access in 2011 as mentioned above in **I (a) 2**.

Article 17 of the Act on Protection of Personal Information requires that "a business operator handling personal information shall not acquire personal information by deception or other wrongful means" but its violation is not a criminal offense as such (above in **1 a**).

b. Subject

There is no penal provision that punishes attacks on a person's digital personality. However, it is generally admitted that such attacks can constitute an indirect violation of a real personality, which may be regarded as the criminal offense of defamation or libel.

(c) Protection against Illegal Content: ICT Related

1. Object

a. Child pornography - images of real or virtual children?

As stated in **I (a) 6**, the Act on Punishment of Activities Relating to Child Prostitution and Child Pornography, and the Protection of Children penalizes various conducts relating to child pornography, including production, provision, import, and export. The act did not originally include offenses using the Internet but introduced new regulations now present by an amendment in 2004. The possession of child pornography is in general punishable only with the purpose of providing it to another. Mere access to and acquisition of child pornography are not criminal offenses in Japan, while some ordinances of local governments enlarge the scope of criminal offenses.[16]

It is not possible for judges to order the deletion of child pornography posted on computer systems, while the Ordinance of Kyoto Prefecture against Child Pornography in 2011 gives the Governor of the Prefecture the authority to order its deletion. Violation of the order is punishable by a fine of not more than 300,000 yen. However, according to Article 19 of the Penal Code, confiscation of any tangible object used in the commission of a criminal offense is possible, including an "object which is a component of a criminal act," an "object used or intended for use in the commission of a criminal act," and an "object produced or acquired by means of a criminal act."

Another special criminal law for the protection of children is the Act on Regulation of Inducement of Children by Means of Business to Introduce Persons of the Opposite Sex through the Internet ("Internet Dating Site Control Act," Act No. 83 of 2003). Articles 6 and 33 of the act penalize inducement of children through the Internet to certain

[16] For example, the Ordinance of Kyoto Prefecture against Child Pornography in 2011 penalizes acquisition of child pornography in exchange for a reward if it was made by means of a sexual crime against a child. (Kanako Takayama, one of the authors of this report, was a drafting committee member.)

prohibited conducts that do not constitute child prostitution but are similar to that (sexual conducts in exchange for a reward). The penalty is a fine of not more than 1,000,000 yen.

The definition of child pornography in the Act on Punishment of Activities Relating to Child Prostitution and Child Pornography, and the Protection of Children is probably different from those in international instruments, since it was made on the basis of national concerns. "Virtual child" pornography is not criminal in any provisions of national and local criminal laws.

Article 2 *(Definitions)*

(3) The term "child pornography" as used in this Act shall mean photographs, recording media containing electromagnetic records (any record which is produced by electronic, magnetic, or any other means unrecognizable by natural perceptive functions and is used for data-processing by a computer; the same shall apply hereinafter) or any other medium which depicts the pose of a child which falls under any of the following items, in a visible way:

(i) Any pose of a child engaged in sexual intercourse or any conduct similar to sexual intercourse

(ii) Any pose of a child having his or her genital organs touched by another person or of a child touching another person's genital organs, which arouses or stimulates the viewer's sexual desire

(iii) Any pose of a child wholly or partially naked, which arouses or stimulates the viewer's sexual desire

Scholars often particularly criticize the definition of (iii) because it is vague and can be interpreted very widely.

In Japan, prostitution as such and its appearance in pornography are not criminal offenses. Therefore, neither children nor adults are to be prosecuted when they are victims of sexual exploitation. In addition, Japanese prosecutors have discretionary power to decide whether to indict a case or not.

b. Any other object where criminalization depends on the use of information & communication technologies (ICT)

Creation and use of true anonymity in order to send and/or receive data in ICT is not a criminal offense unless it constitutes a crime relating to money laundering.

Cyber-bullying, cyber-stalking, and cyber-grooming are not defined explicitly as criminal offenses but can constitute

crimes when related to real personality. Applicable laws include the Penal Code (Article 222 for intimidation, Article 230 for defamation). In some cases, Article 224 for kidnapping of minors was applied to punish cyber-grooming of a schoolgirl who then actually traveled to the offender. Article 225 for kidnapping for the purpose of indecency could apply in some cases. The Act on Regulation of Stalking and Other Conducts (Act No. 81 of 2000) punishes repetition of certain conducts including "the offender telling the targeted person that he/she is watching over the targeted person," "demanding to meet or have other contact," and "submitting information to the person that would cause (sexual) dishonor."

2. Act – creation/accession/possession/transfer/public distribution by ICT

Right now, there is a debate ongoing regarding whether Japan should criminalize the mere possession of child pornography without the purpose of providing it to another. This is a criminal offense in the Ordinance of Nara Prefecture in cases involving children up to twelve years old but many scholars think that the ordnance is unconstitutional. The Liberal Democratic Party submitted a bill to amend the Act on Punishment of Activities Relating to Child Prostitution and Child Pornography, and the Protection of Children in 2013 in order to penalize possession of child pornography for the purpose of arousing or stimulating the possessor's own desire. However, the prospect for the amendment is low because the opposition is quite strong.

(d) ICT-Related Violations of Property, Including Intellectual Property

Computer fraud was introduced into the Penal Code in 1987 as Article 246-2 as mentioned in **I (2) 1**. In the traditional offense of fraud (Article 246), it was necessary to give false information to a person. At the same time, the offense of theft (Article 235) requires that the object be tangible. Therefore, misuse of an online remittance system, for example, was not punishable, which gave cause for this amendment.

Infringement of intellectual property rights and industrial espionage are punished by general provisions including both cases with and without the Internet in the Unfair Competition Prevention Act, the Copyright Act (Act No. 48 of 1970), and other special criminal laws protecting intellectual property rights.

(e) Criminalization of Acts Committed in the Virtual World

In Japan, virtual personalities as such are not protected by criminal laws. Only conducts involving a real personality

can be punished under the present law.

(f) Non-Compliance Offenses

In Japan, there are many non-compliance offenses and the field of cybercrime is no exception. Examples are punishment of violation of an order of a Minister or a Governor such as Article 56 of the Act on Protection of Personal Information mentioned in **I (a) 6** or in the Ordinance of Kyoto Prefecture against Chile Pornography mentioned in **(c) 1 a**. Sanctions are usually criminal fines. Administrative fines are not very common in Japan.

III Complementary Information Concerning Law and Practice

(a) Criminal Statistics

The "White Paper on Crime," issued by the Ministry of Justice every year, has a special section for "High-Technology Offenses." It provides information about the recent general tendency, frequency, prosecution rate, and so on of several crimes.

Among these crimes are: "unauthorized creation and damaging of electromagnetic records, etc." (Articles 157, 161-2, 258, and 259 of the Penal Code), "obstruction of business by damaging a computer, etc." (Article 234-2 of the Penal Code), "computer fraud" (Article 246-2 of the Penal Code), "offenses related to electromagnetic records of payment cards" (Articles 163-2 ff. of the Penal Code), "offenses in the Unauthorized Computer Access Act," "distribution of obscene objects" (Article 175 of the Penal Code), "child prostitution," "child pornography," "offenses in the so-called Internet Dating Site Control Act," "offenses in the youth protection local ordinances of prefectures," and "offenses against intellectual property rights."

The National Police Agency provides more detailed statistics in Japanese.[17]

(b) Websites about Cybercrimes

An English version of the "White Paper"[18] is available on the website of the Ministry of Justice, although the latest version is available only in Japanese.

[17] http://www.npa.go.jp/cyber/statics/h24/pdf01-2.pdf.
[18] http://hakusyo1.moj.go.jp/en/nendo_nfm.html.

The National Police Agency offers some information on child prostitution and child pornography[19] as well as on cybercrime in general[20] on its website in English. It has established a special website "Cyberpolice."[21] Besides, the Ministry of Economy, Trade and Industry offers some information on the protection of trade secrets.[22] The Ministry of Internal Affairs and Communications has a site for information and communications technology.[23]

(c) Victimization Surveys

The "White Paper on Crime Victims" issued by the Cabinet Office offers scarce information on victims of cybercrimes. The only category is "offenses related to electromagnetic records of payment cards" (Article 163-2 ff. of the Penal Code) but obviously most of the victims are companies. Therefore, the statistics of the Ministry of Justice and those of the National Police Agency would be useful.

(d) Frequent Crimes

Although it is said that in the field of cybercrime, the "dark figure" (*Dunkelziffer*) must be relatively large, the general tendency can be understood from the statistics. According to the research of the National Police Agency and the Ministry of Justice, the most frequent offenses are "computer fraud," "child pornography," and "distribution of obscene objects." These are followed by "unauthorized computer access," "violation of intellectual property rights," and other offenses against children.

The number of reported computer viruses is very large but, since *mens rea* of the distributor is not clear, the number is not included in cybercrime offenses as such. The same applies to the "phishing"[24] and illegal interception of computer data.[25]

---

19 http://www.npa.go.jp/english/syonen2/The_situation_of_child_protection_in_Japan.pdf.
20 http://www.npa.go.jp/cyber/english/index.html.
21 http://www.npa.go.jp/cyberpolice/english/index.html.
22 http://www.meti.go.jp/english/press/2011/1201_01.html.
23 http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/index.html.
24 The Council of Anti-Phishing Japan provides monthly report on reported phishing cases: http://www.antiphishing.jp/.
25 The Ministry of Internal Affairs and Communications has been established.

(e) Computer Crimes Units

The National Police Agency and all forty-seven Prefectural Police Divisions have a special unit for combating cybercrime. The scale depends on the population of the prefecture. The Metropolitan Police Department (Tokyo) also has specialized police officers for cybercrime.

The National Police Agency established the High-Tech Crime Technology Division in 1999 to technically assist cybercrime investigation nationwide. Through its initiative, the Cybercrime Technology Information Network System (CTINS) was established in 2001, in which fourteen Asia-Pacific countries participate for annual conferences.

(f) Courses on Cybercrime

In Japan, law schools and faculties of law do not provide special courses on cybercrime. However, all courses on criminology taught at universities and colleges are expected to include description and analysis of cybercrime.

(g) Training of Professionals

There is a brief introduction to the "Cyber Force training system" by the National Police Agency.[26] The Supreme Court and the Ministry of Justice do not have a corresponding training system for judges and prosecutors, but some of them become specialized through their experience in cybercrime cases.

(h) Frequency of Crimes

The recent tendency can be summarized as in the following table.

[26] http://www.npa.go.jp/cyberpolice/english/action03_e.html.

Forms and Means of Cybercrime Occurrence	Occurring Frequently	Occurring Infrequently	Has not Occurred
Online identity theft (including phishing and online trafficking in false identity information)	X		
Hacking (illegal intrusion into computer systems; theft of information from computer systems)	X		
Malicious codes (worms, viruses, malware, and spyware)	X		
Illegal interception of computer data		X	
Online commission of intellectual property crimes	X		
Online trafficking in child pornography	X		
Intentional damage to computer systems or data (obstruction of business)		X	
Computer fraud	X		
Offenses related to payment cards	X		
Data forgery and destruction		X	
Child abuse	X		
Distribution of obscene objects		X	