Preparatory Colloquium
Verona (Italy), *28 – 30 November 2012*
Section I - Information Society and Penal Law

JAPAN*

Masaki UEDA*

I Criminalization

(1) Protected Interests Subject to Cybercrime Punishment

In Japan, computer network systems (including both control of access and data processing) have become the basis of various activities in society. Once they are attacked, many or unspecified persons may be damaged with regard to the secrecy, integrity, and availability of information. Without any restraint on such attacks, people would distrust computer network systems and abandon the use of the proper functions of such systems. Therefore, Japanese law is said to regard "publictrust in the computer network system as a whole" as aprotected interest whose violation will be punished.[1]

(2) Typical Criminal Provisions

(a) Attacks against Information Technology Systems

There are several offenses that can be regarded as those against IT systems themselves.

Penal Code

Article 168-2 (Useof Electromagnetic Recordsto GiveUnauthorized Commands, etc.)[2]

(1) A person who,for the purpose of usingthecomputer 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 thatgives 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,orto 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.

---

* 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.

* J.D. (Kyoto University), Research Assistant at Kyoto University, Japan.

[1] See, e.g.,Takeyoshi IMAI, "Jittaiho no kantenkara,"*Jurist* No. 1431 (2011), p. 67;Noriaki SUGIYAMA and Masayuki YOSHIDA, "Johoshori no kodokato ni taishosuru tame no keihoto no ichibuwokaiseisuruhoritsunitsuite, Part 1,"*Hosojiho*Vol. 64, No. 4, pp. 1 ff. (Commentary to the amendment of the Penal Code in 2011 written by drafting officials of the Ministry of Justice).

[2]Introduced by the amendment in 2011.

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

Article 234-2 (Obstruction of Business by Damaging a Computer)[3]

A person who obstructs the business of another by interfering with the operation of a computer utilized for the business of the 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 giving unauthorized commands or by any other means, shall be punished by imprisonment with laborfor not more than five years or a fine of not more than 1,000,000 yen.

Act on Prohibition of Unauthorized Computer Access

Article 3(Prohibition of Unauthorized Access)

No person shall have unauthorized computer access[4] (to a limited-use network).

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.

(b) Violation of IT Privacy

The Japanese Penal Code does not have provisions toprotect the secrecy of information as such."Unlawful Opening of Letters" (Article 133) and "Unlawful Disclosure of Confidential Information" (Article 134) do not apply tothe area of information and communication technology.

However, there are several special criminal laws in Japan that protect the secrecy of information on computer networks in limited areas. For example, the Telecommunications Services Act (Article 179 (1) and (2)), the Wire TelecommunicationsAct (Article 14 (1) and (2)), and the Wireless Telegraphy Act (Article 109-2 (1) and (2)) protect the privacy of telecommunications, whereas the Unfair Competition Prevention Act (Article 21 (1)) protects trade secrets.

The abovementioned Act on Prohibition of UnauthorizedComputer Access is also one of these special criminal laws.

(c) Forgery and Manipulation of Digitally Stored Data

Punishment of offenses such as data forgery and manipulation was introduced in 1987.

Penal Code

Article 161-2 (Unauthorized Creation and Use 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 thatis 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

[3]Introduced by the amendment in 1987. An English translation of the Japanese Penal Code is available at thewebsite: http://www.japaneselawtranslation.go.jp/law/detail/?re=01&yo=%E5%88%91%E6%B3%95&ft=2&ky=&page=1. However, the current English version does not reflect the amendment in 2011 as of October 31, 2012.

[4] "Unauthorized access" is defined in Article 2 (4).

be created by a public office or a public officer, the offender shall be punished by imprisonment with labor for not more than tenyears or a fine of not more than 1,000,000 yen shall be imposed.

(3) A person who, with the intent proscribed in paragraph (1), puts an electromagnetic record created without due authorization and 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 to committhe crime proscribed under the preceding paragraph shall be punished.

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 punished by imprisonment with labor for not less than threemonths but not more than sevenyears.

Article 259 (Damaging of Documents for Private Use)

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

(d) Distribution of Computer Viruses

Besides the "Use of Electromagnetic Recordsto Give Unauthorized Commands" (Article 168-2 (2)) mentioned above in **(a)**, "Creation and Offer of Electromagnetic RecordstoGive Unauthorized Commands" (Article 168-2 (1)) are also punishable according to the same Article.

(e) Crimes Related to Virtual Identities of Users, e.g., Forging, Stealing, or Damaging Virtual Personalities

In Japan, there are nolegal provisions that protect virtual identities as such. Only attacks against personalities that would lead to real infringement are punishable as traditional offenses such as fraud or defamation.

(f) Other Innovative Criminal Prohibitions in the Area of IC Technology and the Internet, e.g., Criminalization of the Creation and Possession of Certain Virtual Images

Through recent amendments, the following practices have been criminalized:

–"Display"in public of obscene objects as electromagnetic data storage media (Article 175 (1), first sentence of the Penal Code);

–Distribution of obscene electromagnetic records in public through a telecommunications line (Article 175 (1), second sentence of the Penal Code);

–Offer, display, etc. of child pornography

(3) *Actus Reus* and the Object of Criminal Offenses

In Japanese law, typical *modi operandi* in cybercrimes are "unauthorized access" (Article 2 of the Act on Prohibition of Unauthorized Computer Access), "creation," "offer (provision)," and "execution" (Article 168-2 of the Penal Code).

One of the typical objects of offenses is the "electromagnetic record" as defined in Article 7-2 of the Penal Code.[5] It

[5]**Article 7-2** 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.

must be noted that this does not mean information or data as such, or storage media, but a record of information or data on a certain storage medium.

Another typical object is the "computer."

(4) Limitation of Perpetrators or Victims

With regard to offenses against personal or trade secrets, there are certain restrictions on offenders (who should keep the secret) and objects (protected information) as mentioned above in **(2)(b)**.

Some offenses defined in the Penal Code (as mentioned above) can be committed only against limited objects: For example:

–The offense of damaging of electromagnetic records can be committed only against those "in use by a public office" (Article 258 of the Penal Code) and those "concerning rights or duties" (Article 259).

–The offense of obstruction of business by damaging a computer(Article 234-2) can be committed only against "a computer utilized for the business of another" or "any electromagnetic record used by such computer."

–The offense of unauthorized creation ofelectromagnetic records (Article 161-2 (1)) is punishable only with regard to an "electromagnetic record thatis for use in improper administration of the matters of another and is related to rights, duties, or certification of facts."

(5) *MensRea*

Cybercrimes can be punished only when committed with intention (at least with *dolus eventualis*).

(6) Difference between the Definitions of Cybercrimes and Traditional Offenses

The Japanese criminal legislation tends to punish attacks against data processing in a computer network system as a whole, rather than preventing real damage or danger to individuals.[6]

II Legislative Technique

(1) Problems with Respect to the Principle of Legality

In general, Japanese legislation faces difficulties when it intends to criminalize new conduct emerging in developing areas. Since new technologies are invented continuously, clear delineation between criminal offenses and permitted practices is always a problem.

(2) Avoiding Undue Chilling Effects

Therefore, Japanese legislation tries to eliminate undue chilling effects by express exclusion of cases with "justifiable grounds" from punishment or by limiting the scope of offenses with certain subjective elements such as purposes.

However, the Japanese judiciary tends to cope with new phenomena by means of "extensive interpretation" before the legislation sets about changing the law. This tendency may impair the predictability of punishment and thus bring about chilling effects.

(3) Legislative Techniques to Deal with Development

Japanese legislation often uses references to administrative regulations in order to maintain pace with technological

[6] See *supra***(1)**.

progress. Nevertheless, in the field of information and communication, such regulations have not been used. Therefore, the judiciary applies existing penal provisions as widely as possible at first, and it is not until its end that the legislation introduces new laws.

III Extent of Criminalization

(1) Punishment of Preparatory Conduct

By the amendment of the Penal Code in 2011, punishment for obtaining and retaining of an electromagnetic record to give unauthorized commands (Article 168-3) was introduced. Attempt and preparation of other traditional crimes may be applicable. Accomplices can be punished but only when the principal's act reaches the phase of puinishable attempt. Conspiracy does not constitute an independent criminal offense in Japanese law.

On the occasion of this amendment, certain apprehensions were discussed regarding the fact that development or testing of anti-virus software might be included in the definition of new offenses (creation or offer of a record) or that possible production of "bugs" could be regarded as such offenses. Therefore, the term "without justifiable grounds" was inserted during the drafting process, which clarifies the exclusion of such conduct. In fact, such exemption can be interpreted from the provision even without the term.

Further offenses will be explained in the following **(2)**.

(2) Punishment of Possessing Data

(a) Abuse in Electric Commerce

Preparation for unauthorized creation of electromagnetic records of payment cards(Article 163-4) and attempting to do so(Article 163-5) were criminalized by the amendment of the Penal Code in 2001.The new definition of offenses includes obtaining, providing, and storing a unit of information of an electromagnetic record that is encoded in a credit card or another card for the payment of charges for goods or services.[7]The amendment was the result of the necessity to deal with the phenomenon of increasingp urchasesby forged cards made through unauthorized acquisition of information encoded in an electromagnetic record on a card for payment. Since credit cards are often forged through acquisition of electromagnetic data with a device, a so-called skimmer, legislation had already intended to criminalize this phase.[8]

As a subjective element of this offense, the purpose of use in commission of the crime of "Unauthorized Creation of Electromagnetic Records of Payment Cards"(Article 163-2 (1)) is necessary in addition to the objective conduct of obtaining or possessing informationon an electromagnetic record ofa payment card.

(b) Pornography

Since the amendment of the Penal Code in 2011, possession of electromagnetic data storage media and storage of electromagnetic records have been criminalized with regard to pornography (Article 175 of the Penal Code). Mere holding of information as such does not constitute the crime mentioned above in **I (3)**. As *mens rea*, the purpose of distribution with compensation is required.

---

[7] Attempts to obtain and provide are punishable.
[8] Atsushi YAMAGUCHI,*Keihokakuron, 2nd ed.*(Yuhiaku Publishing, 2010), pp. 486, 493.

The amendment intended to clarify the scope of criminal conduct whose punishability was controversial in case law.[9] This provision formerly targeted "obscene documents, drawings, or other objects,"namely, only tangible objects.Obviously, distribution of electromagnetic data as such was not included. Therefore, the Supreme Court ruled that "an obscene object" meant a hard disk of a host computer storing electromagnetic data of an obscene graphic image.[10]

(c) Computer Viruses

Obtaining and storing are punishable with regard to "an electromagnetic recordthatgives 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" and "an electromagnetic or other record that gives unauthorized commands" (Article 168-3of the Penal Code). According to the officials drafting the amendment, this anticipated criminalization was necessary because acquisition and possession of such records enables them to be put to use.[11]

(d) Unauthorized Access

The Act on Prohibition of UnauthorizedComputer Access, after its amendment in 2012, punishesthe 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 storageof such an illegally obtained code for the same purpose (Article 6).

The Act was originally established in 1999 in order to criminalize unauthorized access to computer networksas such. The background to the legislation was the international situation in which all other G7 (Group of Seven)developed countries except Japan had already criminalized this conduct. The punishment was introduced to plug a loophole in the interests of international cooperation in criminal investigation rather than to cope with internal problems.

(3) Criminal Liability of Service Providers

In Japan, so far, there are no provisions that oblige service providers for networks to delete illegal information and punish its omission. Therefore, the criminal responsibility of service providers can come into question only in case where (i) certain information offeredto many or unspecified persons through a BBS (bulletin board system),etc. constitutes a criminal offense and (ii) the provider, etc. can also be regarded as a principal or an accomplice of the crime through his/her commission or omission.Until now, case law has not punished service providers who merely neglected to delete illegal information but only those who actively contributed to committing the offense by starting and running a specialized BBS in order to induce illegal contents to be uploaded as well as by promoting such uploading, etc. The limits of criminal responsibility depend on criteria for criminal omission (*unechtes Unterlassungsdelikt*)and other theories. Accordingly, punishment of a service provider who only offers access to the Internet is unlikely undercurrentJapanese law.[12]

After all, service providers and so on are not required to perform continual surveillance of uploading illegal information in Japan.

---

[9]SUGIYAMA and YOSHIDA (fn. 1), p. 92.

[10] Decision of the Supreme Court on July 16, 2001, *Keishu*[Supreme Court Reporter in Criminal Matters] Vol. 55, No. 5, pp. 317 ff. The Court regarded the offer of the data as "display in public."

[11] SUGIYAMA and YOSHIDA (fn. 1), p. 89.

[12] SeeHitoshi SAEKI, "Provider no keijisekinin," special issue of *NBL* (*New Business Law*) No. 141, pp. 161 ff.

(4) Constitutional Limits of Criminalization

In the context of the Constitution, it is quite common in Japan to discuss the Internet regarding it as a "forum for speech" (or other expression). Consequently, legal control of harmful information such as pornography or defamation often raises the question of the constitutional limits for the sake of freedom of speech. Other aspects have not so far been much discussed.

(5) Specific Criminal Sanctions

In Japan, there no special criminal sanctions targeting cybercrimes.

IV Alternatives to Criminalization

(1) Relationship of Criminal Law to Other Legal Measures

In the area of criminal law, the principle of legality (*nulla poena sine lege*) makes it difficult to apply existing legal provisions elastically. On the other hand, the Civil Code provides for quite a general clause in tort law (Article 709), which makes it possible to impose reparation so far as a person is damaged, even if the case does not fall within the scope of compensation anticipated by the original legislator. Japanese criminal law punishes only intentional conduc tin this area, whereas tort law also applies to negligent conduct and is thus further-reaching. However, Japanese tort law does not aim to punish the offender but to relieve the sufferer. It is only criminal law that takes sanction against offenses.

In administrative law, there are provisions to oblige a business operator handling personal information to "take necessary and proper measures for the prevention of leakage, loss, or damage and for other security control of personal data" (Articles 20 to 22 of the Act on the Protection of Personal Information). [13] The Wire TelecommunicationsAct, the TelecommunicationsAct,and so on authorize administrative authorities to supervise the infrastructure and security of telecommunicationsservices. Theseprovisions show that administrative law aims to regulate the proper management of information, whereas criminal law applies to harmful conduct.

(2) Non-CriminalMeans ofRegulation of Websites

(a) Filtering

In order to protect children from harmful information, the Act on Creation of an Environment for Safe Use of the Internet by the Young obliges telecommunications service providers (ISP: Internet service provider) that enable connection to the Internet through mobile phones or other communications terminals to offer a so-called filtering service so that "information that is open to public inspection through the Internet and is likely to harm sound development of the young significantly" will be blocked (Articles 17 (1) and 18).[14]

"Filtering"means "to sort information open to public access through the Internet according to certain criteria and to restrict users'inspection of information thatis harmful to the young" (Article 2 (9)). In Japan, this filtering is accomplished by a company (NetSTAR Inc.[15]) who collects and sorts URLs (uniform resource locators) on the one hand as well as by mobile phones companies who take the necessary technical measures on the other hand. Thus, regulation is realized

[13] Criminal sanctions can also be finally imposed in case of contravention of administrative recommendations and orders.
[14] There are no criminal sanctions against breach of duty.
[15] http://www.netstar-inc.com/.

mainly by private enterprises.

(b) Other Regulations

There is no general measure to prevent the sending of illegal or harmful information. It largely depends on self-imposed control of service providers, etc.

(3) Self-Protection of Users

(a) Measures against Unauthorized Access

The Act on Prohibition of Unauthorized Access punishes an act of violating control by the manager of access to a network through imputing the identification code or the password of another as well as through sending data or commands to incapacitate the control, on condition that the use of a computer connected to a network is controlled by the manager through granting an identification code and a password against unauthorized connection from another network computer.[16]

Conversely, it can be said that computer users are expected to take necessary measures to control access to the Internet through their own computers.

(b) Sanctions againstUsers

There are no legal provisions that impose sanctions againstInternet users against their omission to take protective measures. Theoretically, it is possible that anofficer of a stock company must take responsibility forhis/her failure to perform the dutiesaccording to the Companies Act.

V Limiting Anonymity

(1) Obligation to Store Personal Data

Japanese law does not oblige service providers or other enterprises to store personal information of users including communications histories. However, it is often the case that the provider does in fact store such personal data for the purpose of business activities such as collecting charges or dealing with complaints. As far as such data exist, request for disclosure of the information sender's personal data is possible (Article 4 of the Act on Internet Service Providers'Limited Liability). Such data may also become the object of disclosure through a court order in the course of criminal investigation.

(2) Obligation of Providers to Register Users

Japanese law has not introduced such an obligation.

(3) Restriction onEncryption

Neither has Japanese law introduced regulations limiting encryption on the Internet. Even suspects cannot be forced themselves to disclose the passwords they use.

VI Internationalization

(1) Territorial Applicability of National Criminal Law

Japanese criminal law basically punishes only offenses committed withinits territory. Punishment of crimes committed

[16]Hisashi SONODA,*Johokashakai to keiho*(Seibundo Publishing, 2011), pp. 29-30.

outside Japan is very narrowly limited (Articles 2 to 4-2 of the Penal Code). Therefore, case law and legal theories interpret these provisions so widely that crimes committed "within the territory of Japan"covercrimes a part of which was committedin Japan, namely, apart either of the act or of the effect ("ubiquity theory").

The Act on Unauthorized Computer Access was amended to punish offenses committed by a Japanese national outside of Japan (Article 8 (2)) according to Article 4-2 of the Penal Code[17] in order to meet the obligation prescribedArticle 22 (3) of the Convention on Cybercrime of the Council of Europe.

(2) Influence of International Legal Instruments

In 2011, Japan amended the Penal Code to criminalize creation of so-called computer viruses and other conduct in order to ratify the said European Convention. The Act for Partial Amendment of the Penal Code and Other Laws to Cope with Advancement of Data Processing introduced into the Penal Code new offenses relating to electromagnetic records thatwould give unauthorized commands and so on(abovementioned Articles 168-2 and 168-3).

(3) Harmonization of Cybercrime Legislation

Although Japan is not a member state of the Council of Europe, it becamea state party of its Convention on Cybercrime on November 1, 2012.

VII Future Developments

The Penal Code of Japan (1907) defines criminal offenses related to tangible objects, particularly by provisions on offenses against property. Therefore, in the Code, intangible property such as information in computers or in the Internet is not protected as such but rather protected as consequence of protection of tangible objects. There is an argument that legislation is necessary to punish "information theft."[18] In any case, it would not be desirable that information itself does not enjoy any protection by criminal law.

As for prevention of cybercrime, the necessity to protect the network system as a whole, which is what sustains the currency of information, is often emphasized and some insist that the Penal Code should protect the network environment itself.[19] Thisargument seems to be parallel to that regardingthe punishment of offenses regarding protected interestsrelated to electromagnetic records giving unauthorized commands.[20]

In the future, it is likely that technologies will develop so much that cyberspace will become independent from real society.The question will thenbe how and to what extent criminal law should protect such interests that exist only within cyberspace. In this case, precise discussion on protected interests will be necessary in order to provideand limit theproper scope ofcriminal law.

---

[17]**Article 4-2** In addition to the provisions of Article 2 through the preceding article, this Code shall also apply to anyone who commits outside the territory of Japan those crimes proscribed under Part II that are governed by a treaty even if committed outside the territory of Japan.

[18]Keidanren(Japan Business Federation), "Kigyo no joho security no arikata ni kansuru teigen" (Proposal) on March 15, 2005. So-called industrial espionage has been criminalized to some extent by the Unfair Competition PreventionAct.

[19] Osamu SAKUMA, "JohohanzaiCyberhanzai" *Jurist* No. 1348, 2008, p. 108.

[20] See, for example, the literature in Fn. (1) and (20), Takuya WATANABE, "Cyber hanzaiwomegurukeiho no ichibukaisei,"*Keijiho*No. 30, 2011, p. 27.