National Report –Japan*

Takeshi MATSUDA, Megumi OCHI, Tadashi IWASAKI

(B) Jurisdictional issues

(1)(a) How does your country locate the place of the commission of a crime in cyberspace?

Article 1 of the Japanese Penal Code provides that the code shall apply to anyone who commits a crime within the territory. It adopts the principle of territorial jurisdiction. Article 2, 3, 3-bis, 4 and 4-bis of the code provide the supplementary rules of jurisdiction for crimes committed outside the territory, such as the nationality principle, protectionism and universalism, specifying the type of crimes to which each rule should apply.

However, no specific rule about the place of commission is provided and there is no special provision for cyber crime. The dominant doctrine claims that the Japanese Penal Code can be applied in accordance with the principle of territorial jurisdiction (art.1) when one of the elements of the crime, in particular, the "conduct" or the "effect" of the crime, takes place within the territory. But some authors claim that the place of commission should not be specified only by the "conduct" of the crime and require the "effect" to take place in the territory in order to apply art.1 of the code.

(b) Does your national law consider it necessary and possible to locate the place where information and evidence is held? Where is the information that one can find on the web? Is it where the computer of the user is physically present? Is it there where the provider of the network has its (legal or factual) seat? Which provider? Or is it the place where the individual who made the data available? If these questions are not considered to be legally relevant, please state why.

As far as jurisdiction is concerned, it is not considered necessary to locate the place where information and evidence is held. So the question if it is possible to locate the place is not relevant at least in the jurisdictional context. To decide on jurisdiction, it is important to locate the place where the conduct or the effect of the crime takes place, not the place where information and evidence is held.

(2) Can cyber crime do without a determination of the locus delicti in your criminal justice system? Why (not)?

In theory, cyber crime can be constituted without determination of the locus delicti because the definitions of the crime do not contain the place of the commission. However, the punishment of the cyber crime cannot be realised without a determination of the locus delicti, as with other types of crime. At least one element of the crime (either the conduct or the effect) needs to take place within the territory to punish the crime under art.1 of the code, unless the supplementary rules on jurisdiction is applied to the crime.

(3) Which jurisdictional rules apply to cyber crime like hate speech via internet, hacking, attacks on computer systems etc? If your state does not have jurisdiction over such offences, is that considered to be problematic?

The jurisdictional rule to be applied to cyber crime depends on the type of crime. The principle of territorial jurisdiction is applied to all crimes, while the supplementary rules, such as the nationality principle, protectionism and universalism are not applied unless otherwise provided.

Hate speech (via internet) is not criminalized in Japan. However, the principle of territorial jurisdiction (art. 1) applies to defamation (not only defamation committed via internet, but generally), which can be punished under art. 230 of the Penal Code. In respect of the crime of unauthorized access (including hacking, attacks on computer systems, etc.), which can be punished under the law against unauthorized access, the law provides that extraterritorial jurisdiction is to be applied on the basis of treaty.

(4) Does your national law provide rules on the prevention or settlement of conflicts of jurisdiction? Is there any practice on it?

There is no rule provided in Japanese penal law for the prevention or settlement of conflicts of jurisdiction. In cases of international conflict with respect to jurisdiction, the settlement is supposed to be done in accordance with the relevant rules of international law.

* 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.

(5) Can cyber crime do without jurisdictional principles in your criminal justice system, which would in essence mean that national criminal law is applicable universally? Should this be limited to certain crimes, or be conditional on the basis of a treaty?

Cyber crime, as is the case with other types of crime, cannot do without jurisdictional principles in the Japanese criminal justice system.

The idea of universal applicability is problematic, because some of the cyber crimes punishable in certain states are considered inopportune to be criminalized in other states (this is especially the case with crimes of obscenity). It can also be against nulla poena sine lege or any other protection of freedom, because one cannot know if the conduct constitutes crime in all the states in the world. Therefore, the idea of universal applicability is not acceptable, unless it is limited to certain crimes or conditional on the basis of treaty.

(C) Substantive criminal law and sanctions

Which cyber crime offences under your national criminal justice system do you consider to have a transnational dimension?

All cyber crime offences can have a transnational dimension because cyberspace does not have borders. However, it does not necessarily mean that all cyber crime offences actually have a transnational dimension: Cyber crime offences can take place also in the national dimension.

To what extent do definitions of cyber crime offences contain jurisdictional elements?

Generally, the definitions of cyber crime offences by themselves do not contain jurisdictional elements. The jurisdiction is decided according to the general jurisdictional rules (art. 1, 2, 3, 3-bis, 4 and 4-bis of the Penal Code).

There are some penal provisions which contain jurisdictional elements. Article 21(4) of the Unfair Competition Prevention Act, for example, provides that some offences against trade secrets, which can be committed via internet, shall also apply to a person who commits the offences outside Japan with regard to trade secrets controlled from within Japan at the time of the fraud, etc., or the act of violating control, or at the time the trade secret was disclosed by its holder.

To what extent do general part rules on commission, conspiracy or any other form of participation contain jurisdictional elements?

The general part rules on commission, conspiracy or any other form of participation, by themselves, do not contain jurisdictional elements. They are supposed to be applied also to crimes committed within the territory.

Do you consider cyber crime offences a matter that a state can regulate on its own? If so, please state how a state may do that. If not, please state why it cannot do that.

Cyber crime offences committed within the territory of a state can be regulated to a certain extent by the state. Even under the principle of territorial jurisdiction, if the conduct or the effect of the crime takes place in a state, theoretically it can be punished by the state. However, in reality, it is impossible or difficult to implement the investigation, if the evidence or the author of the crime finds itself in other state. Cooperation among the states is required to regulate cyber crime offences.

Does your national criminal provide for criminal responsibility for (international) corporations/ providers? Does the attribution of responsibility have any jurisdictional implications?

There is no special provision for criminal responsibility of international corporations or providers. However, there are arguments on the question under which conditions corporations or providers are responsible for cyber crime offences. The dominant doctrine claims that corporations or providers are responsible only when they intentionally omit to delete illegal information or contents.

(D) Cooperation in criminal matters

(1) To what extent do specificities of information technology change the nature of mutual assistance?

The outstanding feature of developed information technology that impacts on the nature of mutual assistance is its speed. Since possession of a communication record is of great importance during the investigation in order to identify the perpetrator, such possession must be done very quickly, since these records are likely to be erased within a very short time. Therefore, the traditional framework of mutual assistance which requires several procedures involving several authorities, such as the Ministry of Foreign Affairs or the Ministry of Justice, would not effectively work in international cooperation in the case of cyber crimes. Another remarkable feature of information technology is that it enables the criminals to commit crimes from a country other than the one in which the effect of the criminal act occurs, without huge criminal groups or rich financial funds. Such an advantage for the criminals dramatically increases criminal acts across borders. In this sense, worldwide cooperation in investigation needs to be established as well as a more flexible approach to mutual assistance.

(2)

(a) Does your country provide for the interception of (wireless) telecommunication? Under which conditions?

The Act on Communication Interception for the Criminal Investigation (the Interception Act) was adopted in 1999, which allows the prosecutors and the police to intercept communications relevant to the crimes which the suspected person uses or is suspected of using, by a warrant by the courts, in order to identify the perpetrator or the circumstance or contents of commission of the crimes, when it is significantly difficult by other methods (art. 3 of the Interception Act). Such exceptional interception can be used to investigate only certain listed serious crimes committed by several persons (e.g. drug trafficking, aiding smuggling, manufacturing of weapons, etc.). Furthermore, art. 35 of the Japanese Constitution stipulates the conditions under which it is possible to infringe on the right of persons to be secure in their homes, papers and effects against entries, searches and seizures, which require a warrant issued by a competent judicial officer.

(b) To what extent is it relevant that a provider or a satellite may be located outside the borders of the country?

Art. 11 of the Interception Act obliges the providers to cooperate with the interception when requested by the prosecutors or the police. However, such an obligation of providers to cooperate is applicable only to the national providers. It is supposed to require consent when the provider is in another state.

As the authority to investigate is limited within the territory of Japan, even though the effect of a crime is observed in Japan, the Japanese prosecutors or police are not allowed to investigate the provider or the satellite which is suspected of being used or involved in the case but that is located abroad, unless there is consent.

(c) Does your national law provide for mutual legal assistance concerning interception of telecommunication? Did your country conclude international conventions on it?

As the conditions in which the interception is allowed are very limited, the possibility of mutual assistance in interception operation is very low. The Act on International Assistance in Investigation and Other Related Matters (1980) provides general rules of international cooperation. Japan is a State Party to the Convention on Cybercrime which provides for mutual assistance in accordance with the national legislation.

(3) To what extent do general grounds for refusal apply concerning internet searches and other means to look into computers and networks located elsewhere?

Assistance is restricted when: the relevant offence is political; the offence would not constitute a crime under Japanese law; and the essentiality of the evidence is not demonstrated in writing (art. 2 of the Act on International Assistance in Investigation and Other Related Matters). With respect to the second restriction, the Convention on Cybercrime to which Japan is a State Party obliges taking all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law upon receiving the request from another Party. But dual criminality shall not be required as a condition to providing such preservation (art. 29 (3) of the Convention on Cybercrime). It is unclear whether the third restriction can be the ground for refusal.

(4) Is in your national law the double criminality requirement for cooperation justified in situations in which the perpetrator caused effects from a state in which the conduct was allowed into a state where the conduct is criminalised?

Art. 2 (ii) of the Act on International Assistance in Investigation and Other Related Matters stipulates that assistance shall not be provided when the act constituting the offence for which assistance is requested would not constitute a crime under the laws and regulations of Japan were it to be committed in Japan, unless otherwise provided by a treaty. In the same vein, if the act is criminalized in Japan but it is not in the other state, Japan is not able to request assistance in the investigation from the other state. It is an issue of concern, for example, that there are still many states which have not enacted the necessary legislation to criminalize unauthorized access. However, with respect to cooperation with the United States, the Treaty between Japan and the United States of America on Mutual Legal Assistance in Criminal Matters makes the double criminality requirement less strict in assistance between Japan and US and allows the parties to investigate on a non-compulsory basis even though the suspected crime is not provided for in the other state's criminal code.

(5) Does your national law allow for extraterritorial investigations? Under which conditions? Please answer both for the situation that your national law enforcement authorities need information as when foreign authorities need information available in your state.

It is understood as a general rule that each state must respect the sovereignty of the other state and that a state cannot exercise its enforcement jurisdiction in the other state unless the other state agrees to accept it. The Japanese Criminal Procedural Code is applicable outside of Japan as long as the other state consents to it. The general rules for extraterritorial investigation are stipulated in Chapter 13 of the Guideline for Criminal Investigation (the Guideline). Unless there is another international treaty, agreement or special rules, the investigation of international crimes (crimes committed by foreigners, crimes committed by

nationals but outside of Japanese territory, crimes concerning embassies or other crimes related to foreign countries) shall be conducted in accordance with the rules in the Guideline (Art. 223 and 224). Generally, the investigation of international crimes is conducted under the control of the Chief of Police (art. 225 and 226). The Guideline recognizes the relevant privileges and immunities of embassy and other foreign officials. Investigations can be conducted within the premises of the embassy, the ambassador or staff of the embassy when there is consent by the appropriate authority (art. 227). Other similar provisions are set with respect to foreign military ships (art. 229), consulates (art. 239) and foreign private ships (art. 231). Being an insular state, investigation in the territories of the other state is not supposed to be conducted in other situations.

(6) Is *self service* (obtaining evidence in another state without asking permission) permitted? What conditions should be fulfilled in order to allow self service? Please differentiate for public and protected information. What is the (both active and passive) practice in your country?

As the Investigation (even on a voluntary basis) amounts to an exercise of state sovereignty and the investigation by a foreign investigative authority in Japanese territory is not permitted as a general rule, Japan refrains also from the investigation by national investigators in another state (as described in (5) of this section) and it is not possible to collect evidence in another state without acceptance by the state in principal.

However, while the collection of public information may be understood to be not likely to infringe state sovereignty so that it is allowed without acceptance by another state, it is regarded that the decision whether such collection amounts to the exercise of sovereignty which requires the acceptance of the other state is left to the other state, and it is better to gain the acceptance. Some exceptions are recognized, as mentioned in (7).

In practice, since it is widely said that Japanese investigators have not conducted any investigative activities such as direct interrogation of suspects or witnesses in another state, self service seems not to have been used.

(7) If so, does this legislation also apply to searches to be performed on the publicly accessible web, or in computers located outside the country?

Art. 32 of the Convention on Cybercrime, to which Japan is a State Party, permits the party to access publicly available (open source) stored computer data without the authorization of another Party, regardless of whether the data is located in another Party, and to access, through a computer system in its territory, stored computer data that is located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system, without the authorization of another Party. This provision is understood as the exception to allow, without permission of the state authority, the collection of data located in another state which usually shall be collected through the procedure of international assistance in the investigation.

(8) Is your country a party to Passenger Name Record (PNR) (financial transactions, DNA-exchange, visa matters or similar) agreements? Please specify and state how the exchange of data is implemented into national law. Does your country have an on call unit that is staffed on a 24/7 basis to exchange data? Limit yourself to the issues relevant for the use of information for criminal investigation.

Japan has not concluded any PNR.

It is possible to exchange data through Interpol when such exchange of data is regarded as being 'cooperation' (art. 18 of the Act on International Cooperation in Investigation) and does not amount to the provision of evidence. As long as it is just an information exchange involving no compulsory measure, communication between the authorities' counterparts as the exchange of administrative information is possible as long as it does not amount to the provision of evidence. The 24/7 contact point is set at the National Police Agency. The direct mandate of the contact point is limited to 'technical advice' and to only 'promote' the 'collection of evidence and provision of legal information' (art. 35 of the Convention on Cybercrime).

(9) To what extent will data referred to in your answer to the previous question be exchanged for criminal investigation and on which legal basis? To what extent does the person involved have the possibility to prevent/ correct/ delete information? To what extent can this information be used as evidence? Does the law of your country allow for a Notice and Take-Down of a website containing illegal information? Is there a practice? Does the seat of the provider, owner of the site or any other foreign element play a role?

As stated above, Japan has not concluded any PNR. The request for assistance with respect to the collection of evidence necessary for the investigation of national criminal cases is communicated by the prosecution or the police via diplomatic route. While there is no specific national provision to allow this, as art. 197 (1) of the Code of Criminal Procedure permits the taking of necessary measures to collect evidence unless it involves compulsory measures, such a request to foreign authority is permitted as one of the investigative measures. Furthermore, it is also possible to use Interpol as a route to ask for cooperation such as providing information and materials necessary for the investigation of criminal cases.

The procedure to be followed when asked to provide evidence by another state and when asked for cooperation by Interpol is provided in the Act on International Cooperation for Investigation. With respect to the US, the request of the US Department of Justice is to be communicated directly to the Japanese Ministry of Law without going through the diplomatic route according to the Treaty between Japan and the United States of America on Mutual Legal Assistance. Art. 28 of the Convention on Cybercrime provides that the requested Party may set out the conditions for cooperation such as (a) keeping the information confidential or (b) not using the information for investigations or proceedings other than those stated in the request. In what way the information obtained through cooperation in the investigation is used as evidence at trials is decided in accordance with the Code of Criminal Procedure. There is no law which allows the authority to warn or close directly a website containing illegal information.

(10) Do you think an international enforcement system to implement decisions (e.g. internet banning orders or disqualifications) in the area of cyber crime is possible? Why (not)?

The realization of an international enforcement system seems difficult, given that against which crimes the internet banning orders or disqualification are conducted varies depends on the circumstances that each state faces.

(11) Does your country allow for direct consultation of national or international databases containing information relevant for criminal investigations (without a request)?

Japan does not have such a system.

(12) Does your state participate in Interpol/ Europol/ Eurojust or any other supranational office dealing with the exchange of information? Under which conditions?

Japan participates in the work of Interpol. The Cybercrime Technology Information Network System (CTINS) was established in 2001 and 14 Asia-Pacific countries participate in it.

(E) Human rights concerns

Which human rights or constitutional norms are applicable in the context of criminal investigations using information technology?

The relevant human rights provisions in the Japanese Constitution are as follows: right to privacy (art. 13 and 35);[1] freedom of thought and conscience (art. 19); freedom of religion (art. 20); freedom of assembly, association and speech (art. 21); prohibition of censorship and right to secrecy of any means of communication (art. 21); right not to be deprived of life or liberty or to be imposed criminal penalty except according to procedure established by law (art. 31); right to access to the courts (art. 32); right not to be arrested without warrant unless apprehended (art. 33); rights to be informed of the charges and access to counsel (art. 34); right to be secure in their homes, papers and effects against entries, searches and seizures without warrant (art. 35); and other human rights protection provisions regarding criminal investigations and trials (art. 36, 37, 38, 39, 40).

Three basic principles protect the rights of people from criminal investigation. The 'principle of proportionality' in investigation is one of the basic principles regulating the methods of investigation and protecting the rights of the suspect and the third party. Another important principle is the 'requirement of warrant'. Art. 35 of the Japanese Constitution provides that "[t]he right of all persons to be secure in their homes, papers and effects against entries, searches and seizures shall not be impaired except upon warrant issued for adequate cause and particularly describing the place to be searched and things to be seized, or except as provided by art. 33. Each search or seizure shall be made upon separate warrant issued by a competent judicial officer." The third principle, stipulated in art. 197 of the Codes of Criminal Procedure, prohibits compulsory dispositions unless special provisions have been established in the Code even if such examination as is necessary to achieve its objective may be conducted.

Japan is a State Party to the main international human rights conventions: the International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Economic, Social and Cultural Rights (ICESCR). Art. 98 of the Japanese Constitution provides that the treaties concluded by Japan and established law of nations shall be faithfully observed. Treaties are understood to be primary to the national laws except to the Japanese Constitution.

Is it for the determination of the applicable human rights rules relevant where the investigations are considered to have been conducted?

Generally, it is understood that the rights guaranteed in the Japanese Constitution are enjoyed by nationals (e.g. Art. 3 of the Japanese Constitution). Foreigners within the territory of Japan would enjoy similar but not equal rights with nationals. The general understanding is that foreigners enjoy the fundamental civil rights and other rights to realize these rights inscribed in the Japanese Constitution, and they do not enjoy the political and social rights. Furthermore, the constitutional rights of foreign

[1] Tokyo district court, judgment, September 28 1964, Case (wa) No. 1882 (1964).

people who are entering Japan are being debated. Therefore, the human rights provided in the Japanese Constitution basically apply within the territory of Japan.

The extraterritorial applicability of international human rights instruments follows the rules of international law.

How is the responsibility or accountability of your state involved in international cooperation regulated?

Japan has ratified the Convention on Cybercrime signed on 23 November 2001. The international obligations of international cooperation are provided in art. 23 to 27 of the Convention. On 5 August 2003, the Treaty between Japan and the United States of America on Mutual Legal Assistance in Criminal Matters was signed and it entered into force on 21 July 2006. With respect to extradition, Japan has concluded the Treaty on Extradition between Japan and the United States of America in 1978 and the Treaty on Extradition between Japan and the Republic of Korea on 3 April 2002.

Is your state for instance accountable for the use of information collected by another state in violation of international human rights standards?

Evidence collected unlawfully may be inadmissible in a criminal prosecution in a court under certain circumstance (exclusionary rule). With respect to testimonial evidence, art. 38 (2) of the Japanese Constitution and art. 319 (1) of the Codes of Criminal Procedure prohibit the use if a confession coerced by way of torture, threat or any other inappropriate means. However, also regarding non-testimonial evidence, even though there are no specific provisions, it is understood to be implied in art. 31 (due process) and 35 (requirement of warrant) of the Constitution and art. 218 (1) of the Code of Criminal Procedure.

It is the general understanding that it depends on the nature of the right infringed when deciding whether to exclude evidence collected in the other state in a manner which infringes the person's rights (e.g. right to silence or right not to be tortured). There is a case concerning the murder of four family members in Fukuoka committed by three Chinese nationals, two of whom were arrested and questioned in China and the testimonies were transmitted to Japan; the courts provide some views on the issue.[2] The case invoked some concerns that there were some differences in measures of human rights protection between China and Japan. However, a rather practical solution was adopted in that the Japanese prosecutor was present at the investigation in China so that all the investigation procedure was conducted in a manner following Japanese criminal procedural rules.

(F) Future developments

Modern telecommunication creates the possibility of contacting accused, victims and witnesses directly over the border. Should this be allowed, and if so, under which conditions? If not, should the classical rules on mutual assistance be applied (request and answer) and why?

Is there any legal impediment under the law of your country to court hearings via the screen (skype or other means) in transnational cases? If so which? If not, is there any practice?

Is there any other issue related to Information society and international criminal law which currently plays a role in your country and has not been brought up in all the questions before?

It may be said that contacting the accused, victims and witnesses directly over the border by using telecommunication should be allowed in view of the principle of direct trial. However, in that case, the relevance to the right to examine a witness (art. 37(2) of the Japanese Constitution) may come into question.

In Japan, Art.157-4 of The Code of Criminal Procedure provides that, under certain conditions, the court may have the witness be present in a place other than the place where the judge and other persons concerned in the case are present for the examination of the witness (limited to the same premises), and examine the witness in a way using devices that allow recognition of the state of the other and communication by transmission of visual images and sound. Such a video link system is allowed for the protection of victims of sexual crimes and the like. However, there is no provision for hearings via the screen in transnational cases in the criminal trial of our country. In order to be allowed to examine in such a way, the guarantee of the right to examine a witness may also be requested. That is a subject for future analysis.

[2] Fukuoka District Court, 19 May 2995, Hanrei Jihou, No. 1903, p.3;Fukuoka High Court, 8 March 2007, Kōtōsaibansyo Keijisaiban Sokuhōsyu (2007), p. 443; Supreme Court, Petty Bench 1, 20 October 2011, Saibanssyo Jihou, No. 1542, p. 360.