Preparatory Colloquium
24 – 27 September 2013, Antalya (Turkey)
Section III: Information Society and Penal Law

JAPAN [*]

Tatsuhiko INATANI [*]

(A) General Question

(1) In Japan, we have no formal or official legal definitions for applications of IT and ICT within the context of criminal procedures, and there are no definitions in Japanese Criminal Procedure Law (herein after JCPL) or the relevant statutes. But in the literature, legislation, and court decisions, the term "jyoho-gijyustu" means IT ("jyoho" means information and "gijyutsu" means technology) or "jyoho-tsushin-gijyutsu" (tsushin means communication). These terms have no precise definition, but are generally used in a situation related to highly sophisticated or developed information technologies. Thus we use those terms within the context of criminal procedures, when subjects or issues relate to highly sophisticated or developed information technologies. When it seems that those technologies may infringe our interests (e.g. privacy), we use these terms to demonstrate the importance of proper reactions to or resolutions of issues with those technologies.

(2) The Japan National Police Agency (herein after NPA) launched a special framework to implement ICT within the criminal justice system. Under the directions of the NPA, local police departments established a cyber force, a special task force to implement ICT, and NPA itself established a cyber force center, the head of the cyber force, to gather and analyze information from each cyber force in

[*] 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.
[*] Associate Professor of Law, Kyoto University

order to improve their activities[1].

(3) Some private organizations provide ICT related services to the Japanese criminal justice system. For instance, anti-virus companies provide analytics and information on unknown computer viruses to the police. But their cooperation is voluntary and not based on any statutes. Thus, law enforcement officials cannot force them to cooperate or share confidential information with them for precautionary activities[2].

(B) Information and Intelligence: building information positions for law enforcement

(1) Although in limited form, data mining is used to build information positions for law enforcement. NPA runs "CIS-CATS," a database of integrated information on the features of crimes (e.g. method, time and location of crime and profile of suspect and so forth) in order to improve the efficiency of activities and the accuracy of decision-making of law enforcement agencies[3].

(2) Law enforcement agencies can access some public databases. For instance, the DNA database, fingerprint database and CIS-CATS. However, they cannot access private databases without a judicially authorized warrant.

(3) The police use data mining, but they do not use the technique to profile potential perpetrators or risk groups. But they could do so through CIS-CATS.

(4) Based on so-called "Tsushin-Boujyu-Ho[4]," law enforcement agencies can intercept telecommunications. But in order to conduct an interception, they have to obtain a judicially authorized warrant. And that warrant requires a higher degree of suspicion than "probable cause" on a particular crime. Thus law enforcement agencies cannot use this sort of surveillance for intelligence-gathering activities.

(5) Private individuals are not obliged to retain information for law enforcement agencies. This issue has caused controversy about the relationship between the right to confidential communication[5] and attempts to fight highly sophisticated crimes in Japan[6].

---

1 *See* NPA, HEISEI 24NEN KEISATSU-HAKUSHO, at 48
2 *See* Sogo-Security-Taisaku-Kaigi, Aratana-Saiba-Hanzai-ni-Kansuru-Kadai-to-Kongo-no-Taisaku-ni-tsuite, at 9-10
3 *See* NPA, *supra* note 1, at 87
4 "Hanzai-Sousa-no-tame-no-Tsushin-Bojyu-ni-Kansuru-Houritsu"
5 §21 art.2 of Japanese Constitution
6 *See e.g.* NPA, HEISEI 23 NEN KEISASTU-HAKUSHO, at 55

(6) Private individuals are not obliged to provide information to law enforcement officials, but if a law enforcement agency officially requests a third party to submit their data, they can provide it[7].

(7) Some methods are under judicial control and others are not. For instance, the interception of telecommunications is under judicial control. But building a DNA database is not under judicial control if the law enforcement agency can obtain the samples without coercion.

(C) ICT in the criminal investigation

(1) Under the JCPL, law enforcement agencies cannot intercept e-traffic data or content data in real time.

(2) Based on §218 art.1 and §218 art.2 of the JCPL, law enforcement agencies can access and search information systems for e-traffic data and content data, but they cannot seize the data itself. In order to secure the data, they copy it to their own medium or more simply they seize a desktop computer, laptop or server as medium. In other words, they can only seize medium not data. And to freeze data, they can ask telecom companies or ISP to preserve the relevant data for 6 months, based on §198 art.3 of the JCPL.

(3) Law enforcement agencies cannot force telecom companies or ISP to share data with them.

(4) Video surveillance is a common method of investigation in Japan. But, a natural person or legal entity cannot be forced to cooperate. If a third party rejects voluntary cooperation, law enforcement agencies must seize their mediums to access or secure the data they need.

(5) Law enforcement agencies may apply audio-visual recording of interrogations. But, they are not obliged to do so, even when they interrogate 'problematic' suspects (e.g. minors, retards or foreigners). This is one of the most provocative issues in the on-going reformation of the Japanese criminal justice system[8].

(D) ICT and Evidence

(1) There are no specific rules on ICT-related evidence in Japan.

(2) There are no rules on the integrity and security of ICT-related evidence, which has led to problems with forged or altered evidence by law enforcement agencies. For instance, in a

[7] §33 art.1 of "Kojin-Jyoho-no-Hogo-ni-Kansuru-Houritsu"
[8] See Housei-Shingikai Shinjidai-no-Keiji-Shiho-Seido-TokubestuBukai, *Dai-13-Kai-Kaigi-Gijiroku*

well-known bribery case, the prosecutors altered the dates of documents in order to eliminate a contradiction in their case.[9]

(3) There are no specific rules on the admissibility of evidence for ICT-related information.

(4) There are no rules on discovery and disclosure for ICT-related evidence.

(5) There are no rules for evaluating ICT-related evidence.

(E) ICT in the trial stage

(1) Although there are no specific procedures for introducing ICT related evidence to a trial in the JCPL, the Japanese Supreme Court held that tapes must be introduced to a trial through a tape player[10]. And in practice, ICT related evidence must be introduced in an appropriate way to reveal its contents[11].

(2) There is no procedure for distant interrogations.

(3) The JCPL does not prohibit the use of digital and virtual techniques for the reconstruction of events.

(4) In many cases, audio-visual techniques are used to present evidence during a trial. In cases judged by a board consisting of Judges and laymen (so-called "saibanin"), the relevant lawyers tend to use audio-visual techniques in order to make their evidence and cases more understandable for laymen. However, the use of such techniques remains controversial because some techniques make so strong an impression that laymen might misunderstand the probative value of evidence or suffer mental stress (e.g. PTSD).

(5) Under the JCPL, it is impossible to replace paper case files with electronic ones, and there are no developments towards digitalizing trial proceedings.

---

[9] This affair is so-called "Osaka-Chiken-TokuSoBu-Shunin-Kenji-Shoko-Kaizan-Jiken", see http://ja.wikipedia.org/wiki/大阪地検特捜部主任検事証拠改ざん事件

[10] *See* Decision of the Supreme Court on March 24, 1960, *Keishu* [Supreme Court Reporter in Criminal Matters] Vol. 14, No. 4, pp. 462 ff.

[11] *See* Matsuo et al., JYO-KAI-KEIJI-SOSHOHO 4TH ED., at 668