Recent Development of Crime Prevention in China: A Japanese Perspective on Data Protection Regime

Nobuhito Yoshinaka*

Abstract

La Chine est devenue l'un des pays les plus développés dans le domaine de la prévention de la criminalité. En particulier, la stratégie de prévention de la criminalité par l'aménagement de l'environnement (CPTED) permet de créer des quartiers plus sûrs. Le gouvernement a défini un cadre de base pour la prévention de la criminalité via sa politique de "gestion globale de la sécurité publique". Ce cadre couvre l'ensemble de la société et constitue une politique de lutte contre la criminalité spécifique à la Chine. Aujourd'hui, le gouvernement mène un nouveau cycle de réforme judiciaire dans le cadre du principe de « the rule of law. » La prévention de la criminalité doit évoluer pour répondre aux besoins de la société et aux exigences de la prévention moderne de la criminalité. Après avoir confirmé la situation actuelle par le biais de la "théorie globale de la prévention de la criminalité", qui se concentre sur la prévention proactive, inactive et réactive, l'auteur examinera les points de vue critiques sur la société de surveillance à partir de l'approche équilibrée du Japon entre sécurité et liberté. La liberté est un travail dans une société sûre. L'auteur souligne le potentiel d'un système de crédit tel que le "Sesame Credit" en tant que mécanisme de prévention de la criminalité.

* Professor of Law, The Graduate School of Humanities and Social Sciences, Hiroshima University, Japan. This note is based on the speech at The Eighth World Forum on China Studies held on 10-11 September,2019 in Shanghai, China.

1. Introduction

China has become one of the safest countries in the world(1). Although academics regard Japan as a safe country concerning crime, statistics reveal that China's crime rate is much lower than Japan's(2).

Given the vast population, approximately fourteen hundred million people living in this country, this is a fantastic outcome despite the different definitions of crimes between the two countries(3). The reasons how China has achieved the target might be as follows.

First, the "Strike Hard" policy has been implemented since 1983 to crack down on illegal activities. This strategy operated in 1983, 1996, 2001, and 2010.

Secondly, what we call, the "Comprehensive Management of Public Security Policy" has been introduced since 1991. This policy is a holistic approach to crime prevention, including various tactics or strategies to deter offending in society. In 2001, *Jiāng Zémín* combined the idea of the rule of law with that of the rule of morals. From 2013 onwards, the leader of the PRC, *Xí Jìnpíng,* has emphasized the importance of the State Ruled by Law.

Lastly, China adopts "The Global Crime Prevention Theory," which consists of three strategies: proactive prevention, inactive prevention, and retroactive prevention. Thanks to this theory's implementation, the murder rate, for example, has dramatically declined in recent years(4). This short note focuses on the proactive

---

（1） *Re* crime and crime prevention since China's new open-door policy, see P C Friday, Crime and Crime Prevention in China: A Challenge to the Development-Crime Nexus, Journal of Contemporary Justice Vol.14 ,296-314, 1998.

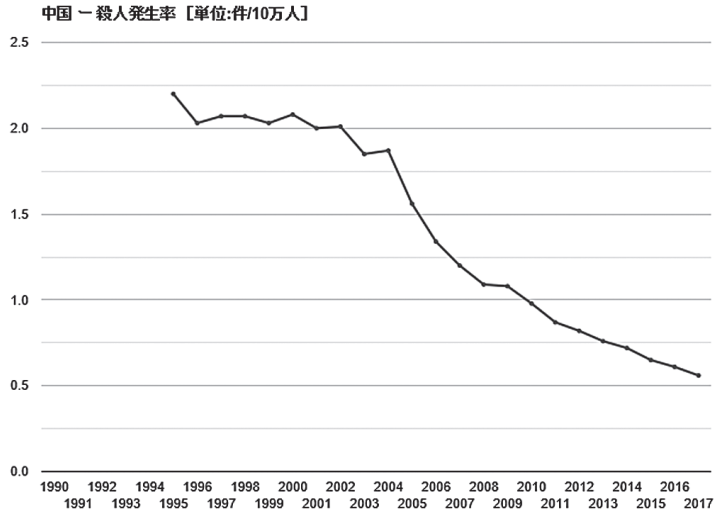
（2） The White Paper on Crime 2016, The China Statistic Yearbook / The China Law Yearbook (2011-2016).

（3） In particular, the minor amount theft does not constitute a crime in China.

（4） In detail, see *Líng Qiū Yáng, Nobuhito Yoshinaka*, A Study of the Status Quo of Crime Prevention in China, The Hiroshima Law Journal, 42(2), 105-138, 2018.

measures and their implications from Japan's point of view.

〔The Murder Rate in China〕 Materials：GLOBAL NOTE/Source：UNODC



2. Proactive Crime Prevention in China

The idea of proactive prevention in China branches into four phases. First, it is called "Situational Crime Prevention." This concept is the implementation of Environmental Criminology in the US. Although this wording *per se*, including CPTED, is not so often used in China, people recognize there are many CCTV or IP cameras set up in the public spaces. Connected with the face authentication system, the contents obtained through these cameras would be admissible as evidence in criminal proceedings and a powerful deterrent effect to potential offenders.

Secondly, the Macro Prevention System of Public Security has started. This initiative consists of building four networks between communities, public spaces, companies, and boundaries between administrative jurisdictions, establishing three mechanisms for information sharing between law enforcement agencies through the

internet, a practical and authoritative command center, and a speedy response system in the Police force. Moreover, strengthen two management pieces regarding the population in the administrative jurisdiction and illegal stuff, including swords, guns, explosives, and drugs.

Thirdly, the Micro Prevention Network between the Police and private sectors has constituted, ranging from community policing organizations under the Police Offices to community cooperation between voluntary crime prevention activities and the Police force (E.g., Public Security Allied Defense Forces), to a variety of activities preventing crimes, for example, door-to-door survey, advertising, patrolling, fieldwork investigation, information transmission from the Police. The function of community policing organizations is to provide the residents with developmental education, grasp the community's current situation, public opinion, and population, organize safer community activities, and maintain public order.

Lastly, schools offer ideological, moral, and legal education to children and young people to enhance their awareness of law and order.

It seems that collecting individual information without limitation may conflict with the privacy right of the persons. We will see the legal system dealing with this problem in Japan.

3. Legal Framework of Data Protection in Japan

In Japan also, surveillance cameras are equipped and widespread in many stores, schools, and communities. According to a widely accepted theory, Article13 of the Constitution of Japan covers the protection of privacy and portrait rights. The Constitution generally protects liberty in private life, while the Supreme Court, on December 24, 1969, authorized infringing on those rights as an exception. Moreover, there are two pieces of legislation, both on the private and public sectors, to regulate these fundamental human rights. These are Act on the Protection of Personal

Information 2003(hereafter referred to as APPI) and Act on the Protection of Personal Information Held by Administrative Organs 2003 (hereafter referred to as APPI-AO).

Furthermore, almost all prefectures have their ordinance or by-law to protect personal information(5). These local governments generally provide an additional guideline in case that private sectors want to set up surveillance cameras in their places(6). Article 2 of the APPI and Paragraph 2 in Article 2 of the APPI-AO define personal information in question(7). The criterion is whether the specific individual can identify. If the photos and videos obtained through surveillance cameras cannot

---

（5） E.g., Hiroshima Prefecture has enacted the “Hiroshima Prefecture Ordinance on the Protection of Personal Information 2004”. See https://ops-jg.d1-law.com/opensearch/SrJbF01/init?jctcd=8A8B97723A&houcd=H416901010053&no=3&totalCount=4&fromJsp=SrMj (accessed on 17.10.21).

（6） E.g., Hiroshima Prefecture has instituted “Hiroshima Prefecture Guideline on installation and operation of surveillance cameras 2018.” See https://www.pref.hiroshima.lg.jp/uploaded/attachment/263032.pdf (accessed on 17.10.21).

（7） Act on the Protection of Personal Information defines the meaning of personal information as follows. See http://www.japaneselawtranslation.go.jp/law/detail/?printID=&id=2781&re=01&vm=02 (accessed on 17.10.21).

Article 2 (1) "Personal information" in this Act means that information relating to a living individual falls under any of each following item:

(i) those containing a name, date of birth, or other descriptions, etc. (meaning any matters (excluding an individual identification code) stated, recorded or otherwise expressed using voice, movement or other methods in a document, drawing or electromagnetic record (meaning a record kept in an electromagnetic form (meaning an electronic, magnetic or other forms that cannot be recognized through the human senses; the same shall apply in the succeeding paragraph, item (ii)); the same shall apply in Article 18, paragraph (2)); hereinafter the same) whereby a specific individual can be identified (including those which can be readily collated with other information and thereby identify a specific individual)

(ii) those containing an individual identification code

(2) An "individual identification code" in this Act means those prescribed by cabinet order which are any character, letter, number, symbol, or other codes falling under any of each following item.

(i) those able to identify a specific individual that is a character, letter, number, symbol, or other codes into which a partial bodily feature of the specific individual has been converted in order to be provided for use by computers

(ii) those characters, letters, numbers, symbols, or other codes which are assigned about the use of services provided to an individual or to the purchase of goods sold to an individual, or which are stated or electromagnetically recorded in a card or other document issued to an individual to be able to identify a specific user or purchaser, or recipient of issuance by having made the said codes differently assigned or, stated or recorded for the said user or purchaser, or recipient of issuance

(3) "Special care-required personal information" in this Act means personal information comprising a principal's race, creed, social status, medical history, criminal record, the fact of having suffered damage by a crime, or other descriptions ,etc. prescribed by cabinet order as those of which the handling requires special care so as not to cause unfair discrimination, prejudice or other disadvantages to the principal.

(4) A "personal information database ,etc." in this Act means those outlined in the following, which are a collective body of information comprising personal information (excluding those prescribed by cabinet order as having the slight possibility of harming an individual's rights and interests considering their utilization method).

(i) those systematically organized to be able to search for particular personal information using a computer;

(ii) besides those outlined in the preceding item, those prescribed by cabinet order as having been systematically organized to be able to easily search for certain personal information.

(5) A "personal information handling business operator" in this Act means a person providing a personal information database ,etc. for use in business; however, excluding a person outlined in the following;

(i) a central government organization;

(ii) a local government;

(iii) an incorporated administrative agency ,etc. (meaning an independent administrative agency, etc. prescribed in Article 2, paragraph (1) of the Act on the Protection of Personal Information Held by Incorporated Administrative Agencies (Act No. 59 of 2003); hereinafter the same);

(iv) a local incorporated administrative agency (meaning a local incorporated administrative agency prescribed in Article 2, paragraph (1) of the Local Incorporated Administrative Agencies Act (Act No. 118 of 2003); hereinafter the same);

remember the particular individual, people may not regard them as personal information. The Diet made essential amendments in 2015 and 2016, and 2020. Moreover, a drastic reform, which occurred in 2021, will come into force shortly.

---

(6) "Personal data" in this Act means personal information constituting a personal information database ,etc.

(7) "Retained personal data" in this Act means personal data which a personal information handling business operator has the authority to disclose, correct, add or delete the contents of, cease the utilization of, erase, and cease the third-party provision of, and which shall be neither those prescribed by cabinet order as likely to harm the public or other interests if their presence or absence is made known nor those set to be deleted within a period of no longer than one year that is prescribed by cabinet order.

(8) A "principal" about personal information in this Act means a specific individual identifiable by personal information.

(9) "Anonymously processed information" in this Act means information relating to an individual that can be produced from processing personal information so as neither to be able to identify a specific individual by acting prescribed in each following item in accordance with the divisions of personal information outlined in each said item, nor to be able to restore the personal information.

(i) personal information falling under paragraph (1), item (i); Deleting a part of descriptions ,etc. contained in the said personal information (including replacing the said part of descriptions, etc. with other descriptions, etc. using a method with no regularity that can restore the said part of descriptions, etc.)

(ii) personal information falling under paragraph (1), item (ii); Deleting all individual identification codes contained in the said personal information (including replacing the said individual identification codes with other descriptions ,etc. using a method with no regularity that can restore the said personal identification codes)

(10) An "anonymously processed information handling business operator" in this Act means a person who provides for use in business a collective body of information comprising anonymously processed information which has been systematically organized to be able to search using a computer for specific anonymously processed information or similar others prescribed by cabinet order as systematically organized to be able to search easily for specific anonymously processed information (referred to as an "anonymously processed information database etc." in Article 36, paragraph (1)). However, a person outlined in each item of paragraph (5) is excluded.

As for the amendments in 2015 and 2016, the revised laws reinforced and expanded the usefulness or availability of personal information, which is somewhat superior to protecting individual rights, and introduced new types of personal information to cover people's action history on location information, for example, obtained through GPS devices. Moreover, it incorporated the notion of "Special Care-required Personal Information" to protect "Sensitive Personal Information" following the GDPR in European Union(8).

In the case of providing a third party with the "Special Care-required Personal Information," there is no provision in APPI-AO 2003 amended in 2016. Administrative organs could offer a third party the information concerned, including criminal and crime victim records, without permission. Furthermore, the APPI 2003 amended in 2015 introduced an idea of anonymous information to facilitate the use of helpful information. Paragraph 8 of Article 2, APPI-AO 2003 amended in 2016, also stipulates "Anonymized Personal Information."

The legislation established "The Personal Information Protection Commission" as an independent committee, which gives guidance, advice, recommendation, order, approval, monitoring, supervision, etc., to "Personal Information Handling Business Operators." It does not have jurisdiction over administrative organs.

The APPI amended in 2020 addresses the balance of personal information between protection and utilization, based on technical innovation, and responds to new risks in conjunction with the increase of global data distribution(9). Six pillars underpin the amended Act. First, the state of individual rights is as follows. (1) The amended Act will relax the requirements to request the cessation of use and erasure of

（8） The idea of "individual identification code" is to identify the specific individual through collecting the action history or location information of an individual.

（9） In detail, see https://www.ppc.go.jp/personalinfo/legal/kaiseihogohou/(accessed 21.10.21)

an individual's claim. These are the cases where the rights or legitimate interests are likely to be harmed.[10] (2) As for the method of disclosure of retained personal data, the Act allows the individual to give instructions, including the offer of electromagnetic records. (3) The Act enables the individual to request disclosure of third-party records relating to the transfer of personal data. (4)Retained personal data, including short-term data to be deleted within six months, shall be subject to disclosure and suspension of use. (5) The Act also excludes from its scope (i) personal data that a wrongdoer has unlawfully obtained and (ii) personal data that opt-out provisions have authorized to offer[11] .

Secondly, the nature of the responsibilities of businesses to protect is as follows. (1) In the event of a leak, etc., which may harm the rights and interests of an individual[12] , the business person must make a report to the Committee, and they must notify the individual. (2) The Act clarifies that the business person must not misuse personal information to facilitate illegal or unjust acts.

Thirdly, a mechanism to encourage voluntary action by businesses is to accredit organizations covering specific areas (sectors) of the companies[13] .

Fourthly, the state of the policy in data utilization is as follows. (1) To promote innovation, the Act creates "pseudonymized information." The Act removes names and other details and relaxes the obligation to respond to requests for disclosure and suspension of use, provided that such proposals are limited to internal analysis. (2)

---

(10)　The current Act protects the right to request in law violations, such as a fraudulent acquisition.

(11)　This is a system that allows the provision of personal data to third parties without the consent of the individual, provided that the offer is stopped after the fact at the request of the individual and the items of personal data to be provided are made public.

(12)　This is limited to leaks of more than a certain number of personal data and to certain types of leaks.

(13)　The current system is set to target all the sectors of the companies.

The Act requires that the provision to a third party of information that does not constitute personal data at the source but is likely to become personal data at the recipient be subject to confirmation that the individual has given the consent.

Fifthly, how the penalty should be is as follows. (1) The Act increases the statutory penalties for breaches of orders by the Commission and false reports to the Commission[(14)] . (2) For the offense of unauthorized provision of databases, etc., and for the fine for breach of order by the Commission, the maximum fine for a legal person shall be higher than for an offender, considering the disparity in financial resources between corporations and individuals[(15)] .

Lastly, the extraterritorial application of the law and cross-border transfers is as follows. (1) Foreign business operators who handle personal information relating to a person in Japan will be subject to a report collection and order secured by penalties. (2) When providing personal data to a third party located abroad, the Act requires the transferring entity to facilitate the provision of information to the individual regarding the processing of personal data.

To respond to a digital society, the Cabinet Secretariat has been exploring a further amendment in 2021[(16)] . The brief outline is as follows. First, the Personal Information Protection Commission seeks to integrate three Acts into unified legislation. These are the Act on the Protection of Personal Information, Act on the Protection of Personal Information Held by Administrative Organs, Act on the Protection of Personal Information Held by Incorporated Administrative Agencies, etc. It will make national standard rules on personal information protection regimes in

---

（14） Violation of the order shall be punishable by imprisonment for a term not exceeding one year or a fine not exceeding one million yen. False reports are punishable by a fine of up to 500,000 yen.

（15） Corporations can be punished by a fine of up to 100 million yen.

（16） In detail, see https://www.ppc.go.jp/personalinfo/minaoshi/ (accessed 21.10.21)

local governments under the unified Act. The Commission will have jurisdiction over the whole system. Secondly, to unify regulations in the medical and academic fields, in principle, public hospitals, universities, etc., will be subject to the same regulations as private hospitals, universities, etc. Thirdly, to comply with the GDPR's sufficiency requirements, including academic research, the Commission wishes to elaborate exemptions for academic research as exceptions for each obligation, rather than uniform exemptions. Fourthly, the Commission wishes to unify the definition of personal information among national, private, and local governments and clarify the rules for handling anonymized processed information in administrative agencies, etc.[17] . The pseudonymized information introduced by the amended Act of 2020 remains in this proposal.

4. The Personal Information Protection Law of 2021 in China

In October 2020, China released a draft of its Personal Information Protection Law (PIPL), which has many similarities to the GDPR (General Data Protection Regulation) in the EU. On August 20, 2021, the 30th meeting of the Standing Committee of the 13th National People's Congress voted to adopt the "Law of the People's Republic of China on the Protection of Personal Information." It came into effect from November 1, 2021. The detailed examination is beyond the scope of this note, and the author points out some crucial issues[18] . (1) This Act is the first legislation called "Personal Information Protection Law," though the Cybersecurity Law and Data Security Law came into effect in 2017 and 2021. (2) The PIPL defines

---

（17） The direction toward the amendment in local governments is: (1) Establishing standard nationwide rules to balance "personal information protection" and "data distribution. (2) to ensure the proper implementation of the Act, the government establishes guidelines.
(3) The Personal Information Protection Commission shall allow the minimum necessary independent protection measures within the limits of the law.

"Personal information" broadly as all information related to identified or identifiable natural persons recorded by electronic or other forms, apart from anonymized information. The Act distinguishes between anonymized information, which does not constitute personal information, and de-identified information, which still includes personal information. Anonymization refers to the processing of personal information that makes it impossible to identify natural persons, and nobody can reverse it. De-identification refers to the processing of personal information that makes it impossible to identify certain natural persons without additional information(19) . It seems comparable to the concept of pseudonymization under the European Union's GDPR. This distinction appears in Japan's legislation also, as mentioned above. (3) Collecting, preserving, storing, processing, transmitting, providing, and disclosing personal information are handling personal data. (4) In the case of handling personal information about individuals in China, the Act will also apply to use outside China. (5) When providing personal information to a third party, it is necessary to inform the individual who is the subject of the personal information of the purpose of use of the personal information by the third party. (6) Some personal information handlers need to store personal information data in China. (7) One of the conditions under which one can handle personal information is obtaining consent from the individual. (8)

（18） In detail, see the Chinese full text shown at https://baijiahao.baidu.com/s?id=1708628055309894611&wfr=spider&for=pc (accessed 21.10.21), Takayuki, Matsuo and Hu Yue at Momo-o, Matsuo & Namba Law Firm, *"Chugoku Kojin Jhoho Hogo Sooan ni Tsuite*," NEWSLETTER-Chugoku, 2020, and Tomas Zhang, "*China's Personal Information Protection Law: Compliance Considerations from an IT Perspective*," China Briefing, 2020 at https://www.china-briefing.com/news/data-privacy-china-personal-information-protection-law-it-compliance-considerations (accessed 21.10.21).

（19） Article 73, (3) states that " 去标识化，是指个人信息经过处理，使其在不借助额外信息的情况下无法识别特定自然人的过程 ," whereas (4) stipulates that " 匿名化，是指个人信息经过处理无法识别特定自然人且不能复原的过程 ."

Even if an individual withdraws the consent, the data subject must not refuse to provide the service. (9) Failure to comply with this Act will result in a fine of up to RMB 50 million (approximately 800 million Japanese yen) or 5% of last year's sales.

5. Concluding Remarks

Regarding domestic crime, people recognize China and Japan as the safer countries in the world. One reason lies in that proactive crime prevention works in both countries. However, it is essential to ensure that the rule of law governs law enforcement because it is prone to infringe on civilians' human rights. If the face authentication system identifies who is who, the legal systems in both countries would regard photos and videos obtained through surveillance cameras as personal information, even though related organs pseudonymize them. Hence the data thereof shall be ruled by the personal information protection laws in both countries. Act on the Protection of Personal Information Held by Administrative Organs in Japan that will converge into a unified Act shortly prescribes administrative organs responsibilities dealing with personal information. Article 33 of PIPL in China also clarifies that this law applies to activities related to State agencies' handling of personal information. The nation should protect the personal data collected in proactive crime prevention more than those obtained after a final guilty judgment because the principle *in dubio pro reo* operates before finalizing the conclusion. In a way, the former information could never relate to a crime. Notwithstanding, legalization on conditions is preferable to law blank. From an economic point of view, the utilization of personal information has excellent potentials, while it could entrench privacy rights.

As the same implication but a different type of information, recent years have witnessed the emergence of the social credit system like ZHIMA CREDIT in China's field of crime prevention. However, it is skeptical that private enterprises introduced

it as a direct means of crime prevention[20] . People who behave well for society can acquire a point resulting in benefits. In contrast, wrongdoers will lose it, suffering disadvantages, such as not purchasing air or high-speed train tickets, etc. It seems this system fairly well controls people's behavior and ushers them into a crime-less society. In Japan, Mizuho Bank has introduced the "J.Score" system, a new type of loan in which an AI score of up to 1,000 points determines the interest rate and credit limit. If this system connects to the carrots and sticks idea, people might behave better than ever before, aiming to grow points.

Thus, a person's acquired points situation belongs to also essential personal information, and the PIPL should protect it as a matter of law. Compared with the face authentication system, the scoring system might be better because it relies on a person's free daily conduct. However, we should enjoy a safer life controlled by Big Brother or a free life frightened by possible daily shootings.That is a problem.

（20） It might be used by people who wish to find a good marriage partner.