Special Report on Important Matters after the Release of the List of Issues (CCPR/C/JPN/QPR/7) by the Human Rights Committee
- Six Digital Reform-Related Laws

June 15, 2022
Japan Federation of Bar Associations

I. Content of Recommendations to the Government of Japan

1. The Government of Japan should take the following measures in relation to the six digital reform-related laws enacted on May 12, 2021 in order to guarantee privacy rights provided for under Article 17 of the International Covenant on Civil and Political Rights ("ICCPR"):

(1) Regarding the Basic Act on the Formation of a Digital Society (hereinafter referred to as the "Basic Act"), the Act on the Establishment of the Digital Agency (hereinafter referred to as the "Establishment Act") and the Act on the Protection of Personal Information (hereinafter referred to as the "Personal Information Protection Act"):

[1] Stipulate the guarantee of the right to control one's own information (which falls under privacy rights) under the Basic Act on the Formation of a Digital Society and the Personal Information Protection Act.

[2] Modify the position of the Digital Agency as an administrative organization as follows:

i) The Digital Agency shall be established as an external bureau of the Cabinet Office, not under the Cabinet.

ii) The head of the Digital Agency shall be the Digital Minister (a Minister of State for Special Missions), not the Prime Minister.

iii) The provision for the obligation to respect the Digital Minister's recommendations shall be deleted.

(2) Regarding the amended Personal Information Protection Act

[1] Amend the amended Personal Information Protection Act to strictly limit the circumstances where administrative organs shall be allowed to use or provide any personal information in their possession for purposes other than those intended, including replacing the expression "reasonable

grounds" under Article 69, Paragraph 2, Items (ii) and (iii) of the Act with a stricter expression such as "designated grounds," etc.

[2] Limit the purpose of the Personal Information Protection Act to "protect an individual's rights and interests," as well as significantly expand and reinforce the organization of the Personal Information Protection Committee from the perspective of protecting personal information.

[3] Strengthen the monitoring and supervisory authority of the Personal Information Protection Committee over administrative organs including national and local governments (hereinafter referred to as "Administrative Organs, etc.") for the protection of personal information as follows:

i) The Act shall be amended to require Administrative Organs, etc., to prepare and publish a personal information file register of personal information files related to criminal investigations and diplomacy and defense and notify the Personal Information Protection Committee of the same in advance.

ii) The Act shall be amended to authorize the Personal Information Protection Committee to conduct on-the-spot inspections of and issue orders to Administrative Organs, etc.

iii) For annual reporting by the Personal Information Protection Committee to the Diet, the Committee shall conduct strict inspections of Administrative Organs, etc., and set forth the details of such inspections in the report to ensure transparency of the inspections.

[4] When standardizing systems, ensure that the "decentralized management" method will be adopted where each Administrative Organ, etc., manages the personal information in its possession, prohibiting the "centralized management" method where such personal information retained by Administrative Organs, etc., will be aggregated at a specific organization to which each Administrative Organ, etc., can access.

(3) Laws, etc., Concerning the Standardization of Information Systems in Local Governments

In promoting the system standardization, etc., legal amendments shall be carried out in a manner to maintain such existing authority of handling related to personal information protection as provided for under the personal

information protection ordinances, etc., enacted by local governments, and prevent privacy protection from diminishing.

2. The Government of Japan should establish a new system to effectively monitor and supervise intelligence agencies.

(1) In addition to the monitoring and supervisory system by the Personal Information Protection Committee, establish a separate independent third-party expert organization for the Cabinet Intelligence and Research Office, the Public Security Intelligence Agency, the SDF Intelligence Security Command, the Security Police, the agency to be established in relation to the "Act on the Review and Regulation of the Use of Real Estate Surrounding Important Facilities and on Remote Territorial Islands" enacted in June 2021 (hereinafter referred to as the "Land Use Regulation Act"), and the Cyber Affairs Bureau of the National Police Agency newly established in April 2022.

(2) Establish a system where such third-party organization as described in (1) above shall confirm by its authority the content of the specially designated secrets, information collected by the abovementioned intelligence agencies, and information standardized by the Digital Agency and aggregated at the intelligence agencies, etc., and may issue corrective recommendations/orders if any inappropriate handling is discovered.

II. Reasons to Call for the Recommendations

1. Six Digital Reform-Related Laws

Six digital reform-related laws enacted on May 12, 2021 collectively refer to the Basic Act, the Establishment Act, the Act on the Arrangement of Related Acts for the Formation of a Digital Society (hereinafter referred to as the "Arrangement Act"), the Act on Registration of Deposit and Savings Accounts, etc., for Prompt and Secure Implementation of Provision of Public Benefits, etc., the Act on Management of Deposit and Savings Accounts, etc., through Use of Individual Numbers Based on Intentions of Depositors/Savers, and the Act on Standardization of Information Systems in Local Governments.

With respect to the six digital reform-related laws, there already was concern at the bills submission stage whether these laws would be sufficient in terms of the protection of individual privacy and personal information. Moreover, despite the bundling of 63

amendment bills, only 50-some hours were spent on deliberation in both the House of Representatives and the House of Councillors in total.

The six digital reform-related laws enacted as described above have the following problems from the perspective of privacy and personal information protection.

2. These laws diminish individual privacy and personal information protection.

It is provided that the purpose of the Basic Act is to contribute to the realization of the sustainable and sound development of the Japanese economy and happy lives for its citizens by promoting policy measures for the formation of a digital society (Art. 1), but it attaches too much emphasis on a convenient happy life of citizens, leading to diminishment of the protection of individual privacy and personal information.

The Basic Act upholds noninfringement of the rights and interests of individuals as its basic principles (Art. 10), and the protection of personal information as its basic policy (Art. 33). However, these are only abstract ideas and policies, and the right to control one's own information is not stipulated. Moreover, under Article 10, the individuals' rights and interests are relativized alongside the rights and interests of corporations and national security. During Diet deliberations, the opposition parties submitted an amendment proposal to stipulate the "right to self-determine the handling of information regarding individuals" as a purpose of the Act, but the ruling party rejected this proposal. Neither the Establishment Act nor the Personal Information Protection Act amended by the Arrangement Act (one of the six digital reform-related laws) stipulates the right to control one's own information.

Considering that those who accept the idea of the right to control one's own information as one of the privacy rights have been on the increase both in judicial precedents and theories in Japan since the enactment of the Personal Information Protection Act and the Act on the Protection of Personal Information Held by Administrative Organs (hereinafter referred to as the "Administrative Organs Personal Information Protection Act") in 2003, the lack of clear stipulation of such right under the Basic Act is problematic in promoting digitalization of Japanese society.

A legal system which does not recognize the right to control one's own information as described above is likely to contravene Article 17 of the ICCPR, and recognition of the right to control one's own information would suit the purport of Article 17 of the ICCPR.

3. The Establishment Act that grants significant authority to the Prime Minister and the

Digital Minister conflicts with the ICCPR.

Second, there are significant problems with the organization and the authority of the Digital Agency. The Establishment Act establishes the Digital Agency as an organization equipped with a powerful comprehensive coordination function (such as the right to make a recommendation, etc.), places it under the direct control of the Cabinet in order to strongly promote the national government's information system, the digital infrastructure commonly used by local governments, My Number (individual numbers), utilization of data, and so on (Art. 2), and provides that the head of the Agency is the Prime Minister (Art. 6, para. 1). Further, a Digital Minister who has the right to make a recommendation to the heads of relevant administrative organs will be appointed (Art. 8), as well as a Chief Officer of Digital Agency (which is a special position) (Art. 11), and so on. It is also provided that the Digital Minister may make a recommendation to the heads of relevant administrative organs when he/she finds it particularly necessary, and the administrative organs must fully respect such recommendations (Art. 8. para. 5). This is an exceptional provision without precedent, other than in the case of the Reconstruction Agency established as a time-limited organization in response to a large-scale disaster.

The position and powerful authority of the Digital Agency, the standardization of information systems, as well as possible abuse of such loose provisions concerning the restrictions of use and provision of personal information retained as discussed below will make it technically possible that personal information retained by administrative organs and local governments, and in particular, information held by the Cabinet Intelligence and Research Office, the Security Police organization, the information analysis organization to be established under the newly enacted Land Use Regulation Act, and the Cyber Affairs Bureau of the National Police Agency newly established in April 2022, etc., will be collected, centrally managed and used under the Prime Minister.

There is a concern that such a situation may bring about a so-called surveillance society, which will not only conflict with Article 17 of the ICCPR, but also lead to chilled freedom of expression guaranteed under Article 19 of the ICCPR and a crisis of democracy.

Thus, the Digital Agency should be established as an external bureau of the Cabinet Office, not under the Cabinet, just like other government organs established under the Cabinet Office (such as the Financial Services Agency, the Consumer Affairs Agency,

etc.), and the head of the Digital Agency should be the Digital Minister as a Minister of State for Special Missions, not the Prime Minister. Further, the provision for the obligation of other government organs to respect recommendations of the Digital Minister should be deleted.

4. The use and provision of personal information including sensitive information (subtle information) for purposes other than those intended should be regulated more strictly.

(1) Issues with the Arrangement Act

The Arrangement Act serves to collectively amend and overhaul the relevant 63 laws. Among others, it integrates three laws related to personal information protection covering the private sector, administrative organs and incorporated administrative agencies, etc., into a single law, as well as establishes common nationwide rules for the systems of local governments, unifies the separate jurisdictions into one under the Personal Information Protection Committee, and further corrects the imbalance in existing legislation in the medical and academic fields.

However, there are many issues with the Arrangement Act in terms of the protection of individual privacy and personal information. In particular, the provision of Article 8 of the Administrative Organs Personal Information Protection Act which stipulated conditions under which the use and provision of personal information were allowed is maintained without change under Article 69 of the amended Personal Information Protection Act. In other words, the provision stipulates the conditions for exceptional use and provision of personal information by administrative organs as the existence of “reasonable grounds(between administrative organizations) and “designated grounds,(between administrative organization and private sector)” allowing a fairly loose sharing of such information. However, currently where information is standardized and digitalization is promoted vigorously, this provision stipulating both “reasonable grounds” and “designated grounds” should have been replaced with a stricter provision, because the risk of personal information, especially sensitive information, being collected without good reason and used for purposes other than the intended purposes by the operation of Article 69 of the Act is increasing as a result of the drive toward standardization even though the legal stipulation remains unchanged.

Originally, prior to the enactment of the Administrative Organs Personal Information Protection Act in 2003, the "Study Group on Legislation for the Protection of Personal Information by Administrative Organs, etc.," presided by the Parliamentary Secretary for Internal Affairs and Communications who recommended the legislation had compiled a report titled "Improvement and Enhancement of Legislation for the Protection of Personal Information Retained by Administrative Organs, etc. - Personal Information Protection in E-Government" on October 19, 2001, in which it stated with respect to sensitive information, "we expect that technical considerations will continue to be made by individual sectors, taking the opinions and requests from citizens, etc., into account," leaving this for future discussion. The committees on the protection of personal information under the Houses of Representatives and Councillors had also adopted similar supplementary resolutions to the effect that "specific laws shall be considered as soon as possible for the protection of personal information for which strict enforcement of proper handling needs to be particularly ensured."

However, although the six digital reform-related laws provide for a mechanism in which personal information including sensitive information is managed centrally under the Digital Agency, no technical considerations have been made by individual sectors on the protection of sensitive information. If these laws are enforced as they are, there is the risk of bringing about a surveillance society where the right provided for under Article 17 of the ICCPR will be violated, as well as a concern that freedom of expression guaranteed under Article 19 of the ICCPR will deteriorate and democracy will face a crisis.

(2) Necessity for Flexible Development of Personal Information Protection Ordinances

Personal information protection ordinances of local governments have been established by such governments based on the autonomy of residents in advance of the national government. Therefore, in many cases, advanced provisions in these ordinances are greater than those stipulated under national laws. More specifically, ordinances have provisions which require deliberation by a personal information protection council before acquiring any sensitive information, recognize personal information of the dead, restrict online connections with external organizations, and so on.

Such independent efforts of local governments should be respected based on the principle of local autonomy guaranteed under Article 92 of the Constitution, and when a local government legislates a personal information protection ordinance, it needs to be guaranteed that such local government may take its own measures of personal information protection in a flexible manner. Such guarantees will ensure the effectiveness of privacy protection stipulated under Article 17 of the ICCPR in accordance with regional circumstances.

However, as a result of the latest amendment of the Arrangement Act, such personal information protection ordinances stipulated by local governments in accordance with their local circumstances will be forcibly standardized under law.

Article 94 of the Constitution guarantees a local governments' right to enact ordinances. Standardization under the law of such ordinances that already existed prior to the law denies the principle of local autonomy guaranteed by the Constitution and unduly restricts their right to enact ordinances, and this will lead to infringement of privacy protection stipulated under Article 17 of the ICCPR.

5. The supervisory authority of the Personal Information Protection Committee needs to be substantially strengthened.

As a result of amendment of the Personal Information Protection Act under the Arrangement Act, the Personal Information Protection Committee currently has supervisory authority over all administrative organs. This is a step forward.

However, the supervisory authority of the Personal Information Protection Committee is limited to demanding provision of data and requesting explanation, conducting field investigations, providing guidance and advice, and making recommendations (Arts. 153-156 of the Personal Information Protection Act). With these limited authorities only, it is not sufficiently effective to confirm the inappropriate use of personal information by administrative organs. In comparison to its authority provided by the Personal Information Protection Act over the private sector, such as the authority to access and conduct inspections of books and documents and other property (Art. 143 of the Act) and to issue orders (Art. 145 of the Act), the supervisory authority of the Personal Information Protection Committee over administrative organs is wholly inadequate.

According to the supplementary resolutions of the Committees on the Cabinet of the Houses of Representatives and Councillors, the requirements of "reasonable grounds"

and “designated grounds” as the conditions for the use of personal information retained by administrative organs for purposes other than those intended or its provision to a third party shall be applied strictly, and the Personal Information Protection Committee shall monitor the appropriateness of decisions made by the administrative organs, etc. However, if the authority of the Personal Information Protection Committee is limited to making recommendations, appropriate supervision is impossible. The guidance and supervision by the Personal Information Protection Committee extend to police information including that of local police, and personal information in general collected by various intelligence agencies, such as the SDF Intelligence Security Command , the Cabinet Intelligence and Research Office, the Public Security Intelligence Agency, and so on. Therefore, thorough guidance and supervision need to be exercised also over the collection of personal information and profiling performed in the name of investigation of specified harmful activities (espionage, etc.) or criminal conspiracies to prevent any abuse of such information for purposes other than those intended or other inappropriate use. From this perspective, the Personal Information Protection Act should be further amended to grant the Personal Information Protection Committee authority to conduct on-site investigations of and issue orders to administrative organs.

Further, the Personal Information Protection Act exempts personal information related to national security, diplomatic secrets, criminal investigations and tax examinations from the obligation to give prior notice to the Personal Information Protection Committee (Art. 74, para. 2, items (i) and (ii)), and also from the obligation to prepare and publish personal information file registers (Art. 75, para. 2, item (i)).

On the other hand, looking at the circumstances of developed countries, such as Germany, the data protection inspector (data protection commissioner) has great authority to conduct on-site inspections with respect to the abovementioned secrets and activities (investigations and examinations), confirm the databases once every two years and demand deletion if any irregularities are found.

Administrative organs including such investigative authorities and intelligence agencies should be subject to regulations through on-site inspections of their personal information databases by the Personal Information Protection Committee. Personal information subject to monitoring by public authorities should be kept to the minimum extent necessary, and a legal system should be established to stipulate the legal authority with which public authorities may collect, retrieve, analyze and use private information

and the method of exercising such authority, and so on.

Furthermore, the existing annual reporting by the Personal Information Protection Committee to the Diet is absolutely inadequate. In order to confirm whether the Committee's supervision is actually functioning, and further if the privacy and personal information of citizens are protected, transparency in the use of personal information needs to be secured through the Committee's annual reporting. Thus, the system of the Personal Information Protection Committee should be designed so that strict and appropriate investigations will be conducted for all administrative organs and detailed reports containing points for future improvement will be submitted to the Diet, along with the expansion of its authority to cover administrative organs.

For such appropriate exercise of its supervisory authority as described above, it is necessary to significantly expand and reinforce the organization of the Personal Information Protection Committee, and failing to make such improvement will lead to a situation which conflicts with Article 17 of the ICCPR.

6. A monitoring system for intelligence agencies is necessary to enhance the guarantee of privacy rights.

First, when promoting digitalization of society, it is necessary to concurrently introduce a legal system to realize an appropriate guarantee of privacy rights that may be threatened by digitalization. However, no consideration was paid in this regard during the process of enacting the six digital reform-related laws. In Japan, technologies for the accumulation of large amounts of data, such as the internet, surveillance cameras, GPS devices, etc., have made significant advancements as elsewhere, along with the establishment of the My Number (individual number) system, and so-called "conspiracy crime" was newly introduced for many crimes under the "Act for Partially Amending the Act on Punishment of Organized Crimes and Control of Proceeds of Crime." Under such circumstances, concerns have been pointed out that monitoring of citizens will be reinforced through the expansion of investigations.

When someone feels that they are being monitored, it will be difficult for him/her to judge autonomously based on his/her own values and beliefs and behave freely to collect information and express opinion. In other words, privacy rights are the foundation for realizing personal autonomy which is a prerequisite for personal dignity, as well as a critical condition for freedom of expression. These are extremely important fundamental human rights which contribute also to the maintenance and development

of a constitutional democracy.

Therefore, for the activities of the Cabinet Intelligence and Research Office, the Public Security Intelligence Agency, the SDF Intelligence Security Command, the police (in particular the security police), and further the analytical institution for the personal information of residents which will be established under the Cabinet Office in relation to the Land Use Regulation Act, as well as the Cyber Affairs Bureau of the National Police Agency newly established in April 2022, etc., it is indispensable to establish legislation that enables a reliable supervisory body, i.e. an independent third-party expert organization separately from the Personal Information Protection Committee, to confirm by its authority the content of the specially designated secrets, information collected by intelligence agencies and information standardized by the Digital Agency, etc., and issue corrective recommendations and orders.

Article 41 of the EU Data Protection Directive on investigative organizations, etc., which came into effect on May 5, 2016 also requires organizations engaged in investigation, crime prevention, intelligence, etc., to establish at least one independent public authority for monitoring compliance with the Directive, and it is stipulated that the data protection organization established under the GDPR may be designated as such a public authority.

In order to realize the privacy protection stipulated under Article 17 of the ICCPR, it is necessary to establish an effective monitoring and supervisory system by an independent third-party expert organization for the activities of existing intelligence agencies in operation, in addition to the Personal Information Protection Committee.

III. Past Opinions of the JFBA

1. Opinion Calling for Necessary Legal Amendments and Proper Operation of Laws in relation to the Six Digital Reform-Related Laws from the Perspective of the Protection of Privacy and Personal Information (December 17, 2021)[1]
2. Opinion Concerning the Standardization and Sharing of Information Systems in Local Governments (November 16, 2021)[2]
3. President's Statement Calling for Careful Deliberation of the Six Digital Reform-

[1] https://www.nichibenren.or.jp/library/pdf/document/opinion/2021/211217.pdf
[2] https://www.nichibenren.or.jp/library/pdf/document/opinion/2021/211116_2.pdf

Related Bills (March 17, 2021)[3]

[3] https://www.nichibenren.or.jp/document/statement/year/2021/210317_2.html