LCQ5: Application of artificial intelligence and protection of personal data privacy

Following is a question by the Hon Charles Mok and a reply by the Secretary for Constitutional and Mainland Affairs, Mr Patrick Nip, in the Legislative Council today (November 13):

Question:

It has been reported that the Hong Kong Police Force acquired systems with facial recognition function several years ago. Some members of the public are worried that the extensive collection and use of facial images and other biometric data by government departments, together with integration of the data from various databases, will enable the creation of personal data profiles or credit scoring systems. On the other hand, foreign countries have put in place legislation to regulate the application of biometric data to prevent members of the public from being subject to excessive monitoring, so as to protect human rights, including privacy. In this connection, will the Government inform this Council:

(1) whether it has studied if the following acts constitute an infringement upon privacy rights comparable to that of interception of communications and covert surveillance: tracking, monitoring and recording the movement and location of a data subject without his/her consent and profiling of personal data through integrating the big data collected from the public domain; if it has studied and the outcome is in the affirmative, whether the Government will (a) widen the definition of "covert surveillance" under the Interception of Communications and Surveillance Ordinance, thereby subjecting law enforcement agencies, in their applying facial recognition and related artificial intelligence (AI) technologies, to the requirement of obtaining authorisation and to the oversight of the Commissioner on Interception of Communications and Surveillance, and (b) prohibit law enforcement agencies from applying such technologies before the law is amended; if so, of the details; if not, the reasons for that;

(2) whether, in reviewing the Personal Data (Privacy) Ordinance, it will make reference to the European Union General Data Protection Regulation and introduce regulation on "automated decision making" and personal data profiling, to the effect that a data subject has the right to object to his/her personal data being used in "automated decision making", and the right to demand from public and private organisations an explanation on the criteria adopted for making the relevant decisions, so as to ensure that the application of facial recognition systems and AI is consistent with the principles of transparency, fairness and respect for human rights; if so, of the details; if not, the reasons for that; and

(3) whether, in formulating the Smart City Blueprint for Hong Kong 2.0, it

will establish guiding principles relating to the ethical standards and privacy protection in respect of AI and data application, and make it mandatory for the Government to assess the human rights implications and pass through an independent ethical scrutiny in its research and development as well as procurement of data analysis-related technologies (including facial and image recognition), and to explain to the affected persons the operating principles of the relevant technologies before applying them, so as to reduce the adverse impacts as far as possible; if so, of the details; if not, the reasons for that?

Reply:

President,

My reply to the different parts of the question raised by Hon Charles Mok, based on the information provided by the Security Bureau, the Innovation and Technology Bureau (ITB) and the Office of the Privacy Commissioner for Personal Data (PCPD), is as follows:

(1) The Interception of Communications and Surveillance Ordinance (ICSO) provides a stringent statutory framework for regulating the conduct of interception and covert surveillance operations by law enforcement agencies (LEAs). Since its implementation in 2006, the ICSO has all along been effective in supporting the operations of LEAs, while striking a balance between maintaining law and order and protecting the privacy rights of individuals.

As to LEAs, any operation that constitutes a covert surveillance operation under the ICSO must be authorised by a panel judge or a designated authorising officer. All applications for authorisation must meet the stringent conditions as prescribed in the ICSO, i.e. the operation must be for the purpose of "preventing or detecting serious crimes or protecting public security", and must meet the "proportionality" and "necessity" tests. Moreover, each stage of the authorised operation is subject to stringent control under the ICSO. The Commissioner on Interception of Communications and Surveillance also monitors the implementation of various requirements under the ICSO by the LEAs concerned.

(2) Alongside with the rapid development of information technology, technological advancement in artificial intelligence (AI), machine learning and other fields has made it easier for organisations to replace human decision-making with "automated decision-making" technology. According to the General Data Protection Regulation of the European Union, a data subject shall have the right to opt not to be subject to a decision based solely on "automated processing", including "profiling", which produces legal effects concerning or similarly significantly affects him or her, save for a few exemptions. From the perspective of safeguarding personal data privacy, personal data privacy is one of the factors for consideration in regulating "automated decision-making". Given that the Personal Data (Privacy) Ordinance (PDPO) is a technology-neutral legislation, data users shall comply with the Data Protection Principles (DPPs) under the PDPO, including the principles governing the purpose of data collection, data security and data use,

regardless of the type of technology used to process personal data. The use of personal data in "automated decision-making" shall also be bound by these DPPs. For instance, data subjects should be notified of the purpose(s) of data collection, such as processing by "automated decision-making", before or during personal data collection. In the PCPD's practical recommendations for data users regarding Privacy Impact Assessment, data users are encouraged to assess the impact of relevant personal data policies and procedures on personal data privacy, and the scope of the assessment should cover data processing cycle analysis and how to avoid or reduce privacy risks, etc. In light of the development of new technologies, the PCPD has provided specific guidelines for various sectors. For instance, in the information leaflets on Fintech previously issued by the PCPD, organisations are advised to develop transparent privacy policies and practices when using big data analytics to assess individuals' financial standing for the purpose of credit scoring, including to inform data subjects their rights with respect to their personal data (such as the right to be informed of the purpose(s) of data collection, and that of data access and correction).

(3) The Smart City Blueprint for Hong Kong (the Blueprint), published by the ITB in 2017, has set out the vision to build Hong Kong into a world-leading smart city. It has put forward more than 70 initiatives under six smart areas, covering the building of digital infrastructure to promote smart city development, service provision by the Government and public organisations, as well as supporting measures to encourage the participation of public and private sectors in building a smart city. The Blueprint is the strategic document for the overall smart city development in Hong Kong. In the course of formulating and implementing various specific measures in the Blueprint, relevant policy bureaux and departments (B/Ds) have to ensure that the implementation and operational details are in compliance with applicable laws and regulations, including relevant provisions for protecting personal data privacy, and to seek timely advice from the Privacy Commissioner for Personal Data. The dedicated Smart City Portal (www.smartcity.gov.hk) also provides channels for members of the public to voice out their opinions and suggestions.

The ITB is now conducting relevant review in conjunction with various B/Ds, with a view to releasing the Smart City Blueprint for Hong Kong 2.0 (Blueprint 2.0) in 2020. In formulating the Blueprint 2.0, the Office of the Government Chief Information Officer (OGCIO) will arrange public engagement activities (such as focus groups) and exchanges with the industries in order to gauge views from the industries and the public on various important issues, such as exploring how to enhance information security and protect personal data privacy when adopting different technologies.

With reference to the latest development in other places, the OGCIO has planned to commence a study in 2020 to work out a set of technical guidelines on the application of AI and big data analytics for internal adoption within the Government, including the handling of ethical and privacy issues arising from such application, in order to assist government departments in planning and applying emerging technologies like AI and big data analytics. The OGCIO will liaise closely with the PCPD in the course of the study.

Thank you, President.