LCQ21: Regulation of productions involving artificial intelligence technologies

Following is a question by the Hon Edward Leung and a written reply by the Secretary for Innovation, Technology and Industry, Professor Sun Dong, in the Legislative Council today (December 18):

Question:

It has been reported that quite a number of Legislative Council Members of Hong Kong and Legislative Assembly Members of Macao have recently received pornographic pictures suspected of being falsified using artificial intelligence (AI) technologies. Their faces appear in such pictures, which fraudsters use for blackmailing. In this connection, will the Government inform this Council:

(1) of the respective numbers, loss amounts involved and detection rates of reported blackmail cases received since the beginning of this year involving the use of AI technologies to falsify voices, photographs or videos; whether there have been changes in such figures as compared with those of the same period last year;

(2) as it has been learnt that in light of the recent development and the characteristics of deepfake technology, fraudsters tend to impersonate senior business executives or well-known political figures in order to enhance credibility, what are the authorities' countermeasures in place, e.g. whether the authorities will, by drawing on overseas experience to establish personality rights for well-known social figures, restrict any unauthorised use of AI technologies to falsify voices, photographs or videos without the consent of the persons concerned; if so, of the details; if not, the reasons for that;

(3) as it has been learnt that some videos produced with deepfake technology will be spread through social media, and advertisements are placed on search engines to boost their popular appeal and search rankings, whether the authorities have explored requiring social media administrators to impose restrictions in this regard, including the requirement to indicate in the videos that they have been produced with AI technologies; if so, of the details; if not, the reasons for that; and

(4) given that the Legislative Council General Election will be held next year, whether the authorities have assessed the possibility of foreign forces using AI technologies to interfere in the electoral process and results, particularly by releasing false information to smear candidates; if assessment has been made and the outcome is in the affirmative, what preparations the authorities have made in this regard, e.g. whether they will

set up a dedicated team for official investigation and clarification to respond to the incidents as soon as possible, thus preventing the spread of misinformation from affecting the election process; if so, of the details; if not, the reasons for that?

Reply:

President,

Having consolidated the information provided by the Security Bureau (SB), the Commerce and Economic Development Bureau (CEDB) and the Constitutional and Mainland Affairs Bureau (CMAB), my reply to the four-part question is as follows:

(1) According to information provided by the SB, from January to November 2024, the Police received a total of three fraud cases involving artificial intelligence (AI) deepfakes, which involved the use of deepfake technology to impersonate company employees to instruct commercial organisations to transfer funds to the accounts of fraudsters, and the use of deepfake technology to conduct online dating to lure victims to invest in cryptocurrencies. The most recent case, occurred in October 2024, was detected by the Police based on intelligence. A criminal syndicate manipulated by a triad society, which used deepfake technology to engage in online dating to lure victims in Hong Kong, the Mainland and other parts of Asia to invest in cryptocurrencies was dismantled. The case involved a total of more than $360 million with 27 persons arrested, including masterminds and key members of the syndicate.

Regarding the number of deepfake videos found or reported on the Internet, the Police have started to compile statistics since November 1, 2023. Up to November 30, 2024, the Police have found and received reports on 21 fake videos impersonating government officials or celebrities on the Internet. At the requests of the Police, the 21 clips have been taken down by the relevant online or social media platforms to prevent members of the public from being deceived. So far, the Police have not received any report from members of the public being defrauded as a direct result of the fake videos.

The Police do not keep statistics on the number of blackmail cases involving pornographic photos. However, the Police have noted that since early November 2024, some people have been crudely altering pornographic images for email extortion, involving more than a hundred victims but without any monetary loss. The cases have been referred to the Cyber Security and Technology Crime Bureau of the Police for follow-up investigation and no arrests have been made so far.

Should crime-related information be found on a social media platform, the Police will take the initiative to contact the platform concerned such that timely action can be taken to prevent social media platforms from being exploited as media and tools for committing crimes.

(2) According to information provided by the CEDB, regarding unauthorised use of a person's indicia of identity by means of deepfake technology, whether it is actionable under different areas of law depends on the actual circumstances and evidence of individual cases and cannot be generalised. When the deepfake content involves unauthorised use of a copyright work, trademark and/or making of a misrepresentation causing damage to one's goodwill, legal actions may be brought on the basis of copyright infringement, trademark infringement and/or common law tort of passing off, depending on the circumstances and evidence of each individual case. For example, a legal action may be brought by a well-known person on the basis of common law tort of passing off in a case where a trader uses the well-known person's voice, image or likeness by means of deepfake technology without consent in the course of marketing and promoting the trader's product or service in such manner and to such extent that constitutes a misrepresentation that the trader's product or service is endorsed or licensed by the well-known person, and such misrepresentation causes or is likely to cause damage to the person's goodwill.

To enhance public awareness of fraud prevention, and of the production of fake videos using the deepfake technology, the CMAB advised that the Office of the Privacy Commissioner for Personal Data has launched a series of anti-fraud publicity activities and videos, which remind the public of the importance of protecting personal data privacy.

(3) Currently, there is no legislation in Hong Kong that restricts or regulates social media platforms or their users from using particular technologies (such as AI technology) to create the information content they publish. However, the relevant content must comply with the existing laws and regulations in Hong Kong, including but not limited to the aforementioned. The Government also encourages social media platforms to actively discharge their corporate social responsibility by establishing their own community and platform codes of conduct, terms of service and privacy policies, as well as measures to tackle inappropriate content, in order to regulate the information content posted by users on the relevant platforms (including accuracy, authenticity, intellectual property, and safety) and mitigate privacy and ethical risks.

(4) As regards election, the Government will endeavor to ensure that public elections are conducted smoothly in a fair, just, honest, safe and orderly manner. The Registration and Electoral Office has all along maintained close liaison with the Police and other law enforcement agencies on electoral arrangements, and has put in place an established mechanism for collecting and analysing intelligence and performing risk assessments, and to take appropriate measures to mitigate risks and hazards as necessary, as well as to draw up various contingency plans to cope with any unforeseen circumstances.

In addition, the CMAB, in conjunction with the Information Services Department and other relevant departments, will set up a rapid response team around the election day for elections in the coming year, to closely monitor and pay attention to various types of information during the election period,

and to swiftly and effectively refute or clarify all kinds of false or inaccurate information or comments, so as to ensure that the election will not be affected.