Lawyers: Safeguards needed for CCTV data

thestar.com.my/news/nation/2026/06/18/lawyers-safeguards-needed-for-cctv-data

Photo: FAIHAN GHANI/The Star

PETALING JAYA: Independent audits and clear rules governing access to CCTV footage are needed to ensure public confidence in surveillance systems with privacy data, say cybersecurity lawyers.

Cybersecurity expert Fong Choong Fook said public concern on privacy arises because people do not know who is accessing the CCTV footage or how it is being used.

“Even though the system’s stated purpose is to protect the public, the lack of transparency creates unease among the public,” he said.

As such, he said the CCTV system requires highly skilled and experienced experts to ensure the footage is safe and not being misused.

He noted that surveillance systems in other countries have been hacked, underscoring the need for continuous security measures.

ALSO READ:

[More CCTVs planned across 15 local councils, says Nga]

“Security is not a one-time exercise. Governments and private organisations often overlook CCTV maintenance and security checks,” he said, adding that independent audits should be conducted annually to assure the public that the systems are properly safeguarded.

CLICK TO ENLARGE

Fong also said CCTV reliability in court hinges on proper implementation and maintenance.

“When presented in court, judges will validate several aspects of its quality before accepting it,” he said.

“For something to be admissible, it must be proven that the footage was obtained from a trusted environment and used properly.

“Any CCTV evidence must show that the system was operational without issues and that the recording can be trusted.”

Cybersecurity lawyer Thulasy Suppiah said when using facial recognition to track suspects, there should be clear rules on when it may be used, who may access the data, how long data is retained, and what independent oversight exists.

“This becomes even more relevant in light of the Data Sharing Act, which facilitates data sharing between public sector agencies.

“While data sharing may improve operational efficiency and public service delivery, citizens will understandably want assurance that biometric and surveillance data are

only accessed on a need-to-know basis, for legitimate purposes, and with adequate safeguards against misuse."

Thulasy noted in Malaysia, the privacy discussion is particularly important because the Personal Data Protection Act does not apply to the Federal Government or state governments.

"As more surveillance systems become integrated and data sharing between agencies becomes easier under the Data Sharing Act, robust governance and oversight mechanisms will be essential to maintain public confidence."

To safeguard CCTV data or to prevent hacking and misuse, she said there should be strict access controls and audit trails and encryption of stored and transmitted footage.

"There should also be independent audits of the system, defined retention periods and criminal and disciplinary penalties for unauthorised access."

She also said that CCTV footage is generally admissible and can be persuasive evidence in court.

"This is particularly when it corroborates other evidence such as witness testimony, forensic evidence or digital records."

However, she said CCTV footage is rarely conclusive on its own.

"The courts will place greater weight on footage where there is a clear chain of custody and proper documentation of how the recording was obtained and preserved.

"Authorities should implement documented chain-of-custody procedures from the moment footage is captured until it is produced in court. This includes tamper-evident storage, cryptographic verification, restricted editing rights, audit logs and secure archiving."

"Any extraction or duplication of footage should be recorded," she said.