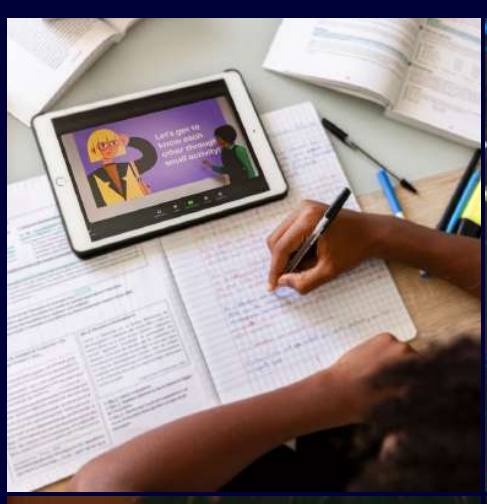
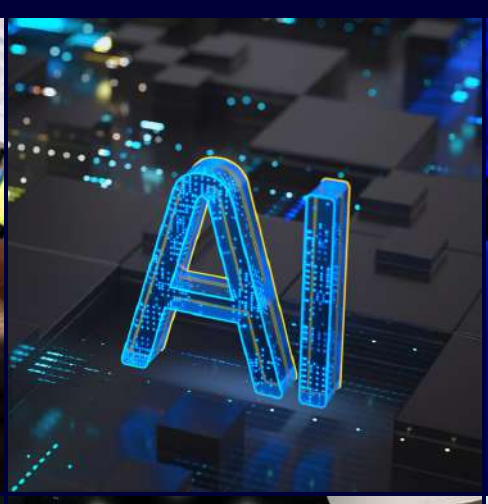
INTERPOL

Innovation SNAPSHOTS

Volume 5 Issue 4 AUG 2025 ▶ Innovation Centre ▶ IC-Snapshots@interpol.int



IN THIS ISSUE

HONG KONG POLICE FORCE'S SMART RESCUE ECOSYSTEM

Search and rescue operations face numerous challenges for law enforcement, such as extreme weather conditions and the safety of responders. Climate change has exacerbated issues of search and rescue for officers, making it essential to develop innovative solutions that enhance public protection, improve rescue efficiency, and shift from reactive to proactive life-saving missions.

However, new and innovative technologies can mitigate these challenges. One such technological innovation is Hong Kong's HKSOS Smart Rescue Ecosystem. This technology provides an integrated solution for enhancing public protection and improving rescue efficiency across diverse situations, shifting from reactive to proactive missions.

The HKSOS Smart Rescue Ecosystem does not rely on mobile connections or satellite coverage. It combines the best features for performance in rescue missions, including a unique accident detection alert system supported by RescueAI.

When the app detects abnormal climate conditions backed by historical data, it automatically alerts the user and emergency services, making it a life-saving tool that reduces rescue response time. The app directly connects to the 999-emergency response centre, ensuring that help is dispatched quickly and efficiently. HKSOS is designed for various rescue scenarios, including sea rescue, mountain rescue, and other emergency situations. The app uses AI to constantly calculate weather conditions, changes in speed, elevation, and other factors, sending alerts to the 999-report center whenever danger is detected. With over 140,000 downloads so far, HKSOS has proven to be a valuable tool in emergency situations.

The technology is integrated with drone systems, allowing mobile phone alarms to alert rescue ground duties even in low-visibility conditions. The drone can also detect signals from individuals in distress, even if they are buried underground.

Looking to the future, Hong Kong aims to establish a global coalition for international assistance, providing a unified platform for rescue missions and emergency response.

The INTERPOL Innovation Centre discussed this application with the support of the Hong Kong Police Force during a webinar held on 18 June 2025 entitled “Smart Safety: Leveraging AI-Driven Mobile Apps for Public Protection”.

Sources: The Government of Hong Kong Special Administrative Region website; Hong Kong Police Force; SCMP.com; INTERPOL Innovation Centre Webinar presentation by Mr Mohammed Swalikh, Senior Superintendent of Police, Hong Kong Police Force.

DIGITAL FORENSICS EXPERTS EXPLORE AI, DEEPFAKES, AND EVOLVING DIGITAL THREATS

The 10th INTERPOL Digital Forensics Expert Group (DFEG) meeting was held in Hong Kong, China from 14 to 16 July 2025. Co-organized by the University of Hong Kong (HKU) and the Cyber Security and Technology Crime Bureau of the Hong Kong Police Force, the event brought together digital forensics and cybersecurity professionals from law enforcement agencies, academia, and industry worldwide.

Experts exchanged insights on emerging techniques in mobile and device forensics, investigative methodologies, and real-world digital forensics case studies from law enforcement agencies. This year, the DFEG meeting was held in conjunction with the 2nd International Digital Forensics Challenge, an annual team-based digital forensics competition for digital forensics practitioners and students organized by HKU and the Hong Kong Police Force.

As a continuation from the 9th DFEG meeting held in Edinburgh, Scotland last year, a key area of interest for the 10th DFEG meeting was the application of AI and large language models (LLMs) in digital forensics tools and investigations. The agenda reflected the growing integration of AI and LLMs into investigative tools and practices, which further highlighted the shift in operational capabilities shared by law enforcement agencies and digital forensic solutions providers globally.

Various presenters examined the use of AI and LLMs in areas such as cryptocurrency analysis, automated evidence processing, and investigative decision support. Practical demonstrations and case studies illustrated how LLMs can assist in interpreting digital artifacts, managing large data volumes, and uncovering complex criminal activity.

Multimedia forensics received significant attention, particularly in response to the increasing use of easily accessible tools to generate synthetic media that has resulted in the proliferation of deepfake content. Discussions covered recent advancements in audio and image authentication, the detection of deepfakes, and the challenges of applying these techniques under evidentiary standards in real-world settings. Mobile forensics also featured prominently, with sessions highlighting the forensic examination of increasingly popular devices such as smart glasses and wearables, along with advances in mobile data extraction, security bypassing, and the recovery of evidence from volatile memory and physically compromised devices.

Lastly, law enforcement representatives shared operational insights from major investigations, emphasizing the importance of adaptability and continuous capability development in response to rapidly evolving digital threat landscapes. Several initiatives that were shared support investigator training through scenario-based simulations and collaborative knowledge development.

INTERPOL’s role in supporting digital investigations was highlighted through updates from the Digital Forensics Lab of the Innovation Centre and the Cybercrime Directorate. These sessions underscored INTERPOL’s commitment to enhancing global digital forensics capabilities and to foster international cooperation to fight transnational cybercrime and to address new and emerging technologies.

Moving forward, an AI in Digital Forensics event will be held in Tokyo, Japan, in October 2025 as part of Project SynthWave, an initiative to develop capabilities for law enforcement to detect AI-generated synthetic media and counter the threats posed by this technology.

INDONESIA’S NEW REGULATION: CHILD SAFETY IN THE DIGITAL AGE

Indonesia’s Government has introduced a new framework (GR17) for safeguarding child protection. Effective March 2025, Indonesia has applied a regulation to strengthen cybersecurity for children, targeting both public and private Electronic System Operators (ESOs) across all platforms, particularly those designed for children.

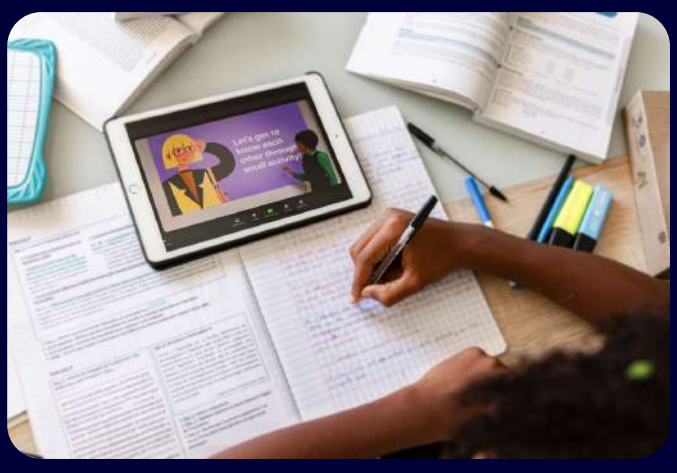
A two-year transitional period has been granted for ESOs to comply with GR17 mandates, which include several obligations such as specifying age categories, implementing child user verification systems, establishing mechanisms for reporting misuse, and ensuring that parental or guardian consent is obtained.

ESOs must also configure high-privacy default settings, conduct personal data protection impact assessments, and provide clear, accurate, and non-misleading information. They are required to offer age-appropriate functionalities, educational content, and responsible notifications for activity or location tracking, while appointing dedicated officers for child data protection.

A critical component of the regulation is a self-assessed risk categorization system, requiring ESOs to classify their products or services as high or low risk based on exposure to harmful content, interaction with unknown individuals, exploitation, and threats to wellbeing.

These self-assessments must be reported to the Ministry of Communication and Digital Affairs, which will verify and assign official risk profiles. Additionally, the regulation encourages public participation in child protection by promoting education and allowing the community to report violations.

Source: Global Compliance News.



DID YOU KNOW?

Argentina created an "Artificial Intelligence Unit Applied to Security" (UIAAS) established under the Ministry of Security. This unit will operate within the Cybercrime and Cyber Affairs Directorate, leveraging artificial intelligence to prevent, detect, investigate, and prosecute crimes. The UIAAS has many functions, including patrolling social networks to investigate crimes and detect security risks, analyse security camera images using facial recognition, use machine learning to predict future crimes, utilize drones for emergency response, and to detect suspicious financial transactions. The UIAAS will operate in accordance with the guidelines and directives established by the Ministry of Security, ensuring compliance with the Personal Data Protection Law.

Sources: Compliance Latam; Brookings Institution.

SWITZERLAND'S NEW APPROACH TO SECTOR-SPECIFIC AI REGULATION

The Swiss Federal Council published their approach for regulating artificial intelligence in Switzerland. In February 2025, the council announced that rather than a cross-sector, general-purpose AI lab, Switzerland will maintain its sector-specific regulatory framework. In accordance with this new approach, overarching regulations governing AI will be applied to areas involving fundamental rights.

Based on the challenge that Switzerland does not currently have a legislative framework for regulating AI, the Federal Council has opted for a sector-specific regulatory approach rather than a horizontal, cross-sector AI regulation applied for all industries. The objective is to maintain Switzerland's position as a hub for innovation, while ensuring the protection of fundamental rights and improving public trust of AI. The roadmap for this approach has been laid out in corresponding measures.

Source: Lenz & Staehelin

Firstly, the Council of Europe's AI Convention will be implemented in Switzerland, and the necessary legislative amendments should be primarily on a sector-specific basis, whereas cross-sectoral regulation should be limited to areas relevant to individuals' fundamental rights, such as data protection. Lastly, parts of the Council of Europe's AI Convention should be implemented through non-binding instruments, such as agreements providing for self-certification of signatories. This approach outlines how AI will be regulated in Switzerland as a whole, and how countries are adopting various AI strategies for this regulation.

SAVE THE DATE: UPCOMING INNOVATION CENTRE WEBINARS

4 Sep	Digital Forensics Series: **OSINT in Digital Forensics**
2 Oct	3D Scanning/Mapping/Photogrammetry Series: **Use of 3D Mapping in Courts**
6 Nov	AI in Digital Forensics Series: Session 7
19 Nov	Data Driven Cities Series: **AI-Driven Surveillance - Unlocking the Power of Advanced Technology in Law Enforcement**
26 Nov	Emerging Technologies Debriefing Series: **Blockchain Malware Detection Tool**

Please contact your INTERPOL National Central Bureau for registration information.

DID YOU KNOW?

Static synthetic voice watchlists have been used across industry and law enforcement to help recognize synthetic voices in impersonation or social engineering attacks. However, biometrics and identity assurance software are developing rapidly and becoming more adaptive.

A patented technology by digital identity company Daon reimagines voice watchlists by combining behavioural, contextual, and voice data. Unlike static watchlists, this system evolves with emerging fraud methods, enabling real-time identification of anomalies associated with synthetic voices. High-risk scores automatically initiate reviews or suspend transactions, acting as an early warning system for suspicious activities.

Source: Biometric Update.

INTERPOL

CALL FOR CONTRIBUTIONS

Spotlight your innovations

- Law enforcement is evolving at an unprecedented pace, fueled by technological innovations and collaborative efforts that redefine policing.
- The Innovation Snapshots newsletter captures and showcases these transformative advancements and invites you to join the conversation.
- We welcome stories from law enforcement, industry innovators, and academic researchers that showcase technologies and novel approaches to drive advancement together.

Submission Guidelines

- Keep contributions to ~400 words.
- Include relevant, high-quality photos with usage rights and credits.
- Maintain a neutral and factual tone.
- Email your contribution to IC-Snapshots@interpol.int and a brief bio of yourself or your organization.

INTERPOL Innovation centre | **@INTERPOL_IC** | **IC.INTERPOL.INT** | **innovation@interpol.int**

INTERPOL

INTERPOL Innovation Centre
INTERPOL Global Complex for Innovation
18 Napier Road
Singapore 258510