Privanova
Research & Consulting

UNODC - JOINT CONSTRUCTIVE DIALOGUE ON TECHNICAL ASSISTANCE AND INTERNATIONAL COOPERATION

Farhan SAHITO, Privanova - speech transcript

07/06/2024 | UNODC, Vienna

CONTACT

privanova.com

contact@privanova.com

34, avenue des Champs-Elysées, 75008 Paris, France

Introduction

On June 7, 2024, the UN Office on Drugs and Crime (UNODC) hosted the Joint Constructive Dialogue on Technical Assistance and International Cooperation in Vienna. This prestigious event gathered representatives from 193 United Nations Member States and observing organisations, underscoring its global significance in addressing critical issues related to crime and justice.

Farhan Sahito, partner at Privanova, had the honour of speaking at this prestigious event. During Panel 3 of the dialogue, Farhan Sahito shared valuable insights on how technology can enhance international cooperation in criminal matters.

Panel III

The role and impact of technology on international cooperation in criminal matters: opportunities, challenges and capacity-building needs

Question

Technology-based tools can be useful entry points for addressing crime-related threats. However, caution is needed in the specific application of these tools to ensure responsible and ethical use and avoid unintended consequences. This is particularly important given that many of the present and future technologies may have serious implications for personal privacy and civil liberties. Could you please share your views on how to monitor and understand the risks posed by the malicious use of technologies and promote ethical standards in the use of these technologies for international cooperation purposes?

How important is, in this regard, the development of multidisciplinary and multisectoral approaches that integrate legal and technical safeguards, as well as oversight mechanisms to ensure compliance with fundamental rights and freedoms?

Farhan Sahtio

Good afternoon, dear colleagues and fellow panelists,

Thank you, Madam Co-Chair, for providing Privanova the opportunity to discuss these critical topics today. Allow me to briefly introduce myself: I am Farhan Sahito, representing Privanova. We are a Paris-based company specialising in R&D at the intersection of privacy, technology, and policy, with a strong focus on law enforcement and cybersecurity.

You have asked two questions, and I will answer them one by one.

Regarding your first question, I agree that using technology-based tools to address criminal threats may have serious implications. For instance, facial recognition technology is useful for identifying suspects; however, these tools have been criticised for inherent biases and potential misuse. A recent case involved the wrongful arrest of Robert Williams when facial recognition technology incorrectly flagged him as a robbery suspect. The police relied on unclear video footage, comparing it to his driver's license photo, but he was innocent and actually driving home from work at the time. This case reveals important privacy concerns about the use of such technology, especially regarding the risk of mistaken identity and mass surveillance.

Another example is predictive policing. These tools help law enforcement agencies analyse crime data to forecast where crimes are likely to occur, allowing police to allocate resources more effectively. However, predictive policing algorithms often use biased historical data, which can result in over-policing marginalised communities. The famous case of Elijah Pontoon illustrates this issue, highlighting concerns about racial profiling.

A third example is drones, which are used for surveillance and tracking criminal activities in real-time. However, the use of drones raises issues concerning privacy invasion, as they can capture images and videos without individuals' consent, and there is potential for misuse by both law enforcement and private entities.

Fourthly, police agencies use cybersecurity tools to detect and prevent cyber crimes and protect important data. However, these tools can involve intrusive measures like deep packet inspection, which can compromise personal privacy.

Another prominent example is social media monitoring by law enforcement agencies to detect criminal activities and gather intelligence. However, this practice raises significant privacy issues, as it involves extensive surveillance of individuals' online activities, impacting free speech and civil liberties.

Now, regarding your question on how to monitor and understand the risks posed by these technologies, several strategies, in my view, can be adopted:

Firstly, legal compliance is non-negotiable. I believe that every use of technology must meet international privacy and data protection laws to protect fundamental rights such as privacy, freedom of expression, and freedom from discrimination. In this regard, developing universally accepted ethical standards for the use of digital technologies is crucial. These guidelines should align with international human rights standards and privacy laws and must be considered from

the initial design phase of technological tools to ensure that personal data is protected.

Secondly, enhancing transparency and accountability is necessary. In this regard, global AI governance initiatives are significant. For example, the European Union's AI Act aims to regulate AI systems based on their inherent risks, which is a big step toward ensuring AI development respects human rights and transparency.

Thirdly, promoting awareness and education is essential. It's crucial to inform the public about the risks and ethical issues of new technologies and their rights concerning data privacy. In addition, training law enforcement and other stakeholders on the ethical use of technology is also vital for ensuring responsible practices.

Regarding your next question on the importance of developing multidisciplinary and multisectoral approaches, I'll break this down into two parts.

First, I'll explain the importance of multisectoral approaches. I believe these approaches are crucial because they bring together diverse perspectives and expertise from various fields, ensuring that criminal matters and complex issues like cybercrime are tackled from all angles. By involving stakeholders from law enforcement, industry, academia, and civil society, we can create solutions that are both comprehensive and effective.

At Privanova, we have witnessed the power of these approaches firsthand through our involvement in EU Commission projects such as ELOQUENCE, SECURE-EU, and CONVERT. One key example includes our work on the POLIIICE, CYBERSPACE, TRACE, and SAFEHORIZON projects. Under these projects, we lead the LEA Cluster, which encompasses over 35 initiatives focused on combating cybercrime and promoting crime prevention. By integrating expertise from academia, industry, law enforcement, and policy-making, these projects effectively address the challenges of cybercrime and crime prevention. In this regard, the EU Commission plays a vital role by providing essential funding, support, and coordination to facilitate international collaboration.

Now, let's talk about multidisciplinary approaches:

First, we must strengthen legal frameworks. This means creating clear legal bases for data sharing and processing, especially for protecting sensitive data and vulnerable groups. We must ensure that all technology use and data processing activities comply with these standards.

Secondly, legal safeguards are essential to align technology use with international human rights standards and data protection laws. Enhancing technical safeguards is also necessary, which means implementing robust data protection measures like encryption, access controls, and regular audits to ensure data integrity and confidentiality. In this regard, the European Union's General Data Protection Regulation (GDPR) sets a high standard for data privacy, which can serve as a model for ensuring that data collected and analysed through technological means is handled responsibly.

Establishing oversight mechanisms is another critical step. Independent oversight bodies are essential for monitoring compliance, investigating breaches, and enforcing corrective actions. They provide accountability and ensure that technology use adheres to principles of necessity, proportionality, and legality.

In conclusion, it is a collective responsibility to ensure that technological advancements serve the greater good and do not compromise the values and principles that underpin our democratic societies. Thank you very much.

Privanova

Research & Consulting