



# IAP

**27<sup>th</sup> ANNUAL CONFERENCE &  
GENERAL MEETING  
TBILISI, GEORGIA  
25-29 SEPTEMBER 2022**

## CALL FOR SPEAKERS

The IAP invites proposals from those interested in giving a presentation during the plenary sessions and workshops of the 27th Annual Conference and General Meeting, during September 25-29, in Tbilisi, Georgia.

The proposal should contain a short description of the proposed presentation or workshop concept for consideration by the Professional Programme Team.

### CONFERENCE THEME

The conference theme is **Global Phenomena Reshaping Criminal Justice Systems**.

The conference will look at the impact of the pandemic on criminal justice systems and examine whether the strategies and digital technologies deployed to ensure business continuity are both desirable and sustainable in the long term. It will look at the rapid growth in the prevalence and sophistication of cybercrimes and the enormous challenges these bring to criminal justice actors. The conference will examine prosecutorial responses, including engagement with the private sector and information technology solutions. It will further explore the forensic capacity, resources, legislative and organizational solutions of prosecution authorities and the role of the private sector in the preservation and recovery of digital evidence. As with evidence, there has been a substantial rise in the number and value of digital assets - the conference will explore the role of prosecutors in national money laundering risk identification and mitigation with a focus on virtual assets, the essential investigative techniques, strategies, and best practice for investigating, seizing, and confiscating virtual assets.

### PLEASE NOTE THE FOLLOWING INSTRUCTIONS

- Deadline for submissions is **31 March 2022**
- The working language of the conference is English. Simultaneous interpretation into French, Spanish, Russian, Arabic and Chinese will be available for all plenary sessions and for selected workshops.
- All proposals must be in English.
- Presentations illustrated with operational outcomes at an international, national, organisational and/or individual case level are particularly welcome.
- **All speakers and other active contributors to the conference must pay a registration fee.** All speakers will however be eligible for the early bird rate throughout the conference registration period.
- If you have any questions, you are welcome to contact the IAP Secretariat at [iap2022speakers@iap-association.org](mailto:iap2022speakers@iap-association.org)

**SUBMIT YOUR PROPOSAL**

**NEXT PAGE: PLENARY SESSIONS SUB-THEMES AND WORKSHOPS**



## **PLENARY 1 Covid, Institutional Challenges & Responses**

**WORKSHOP 1A** Digital transformation across Criminal Justice Systems

**WORKSHOP 1B** Public Health Responses to Crime

## **PLENARY 2 Evolution of Cybercrime Typologies**

**WORKSHOP 2A** Prosecuting Crimes on the Darknet

## **PLENARY 3 Challenges of E-evidence across Borders**

**WORKSHOP 3A** Challenges of Obtaining Electronic Evidence from Abroad

**WORKSHOP 3B** Freedom of Expression & Social Media

## **PLENARY 4 Money Laundering through Virtual Assets**

**WORKSHOP 4A** Parallel Financial Investigations in Practice

**WORKSHOP 4B** Tracing, Seizing & Freezing Virtual Assets



## PLENARY 1

### Covid, Institutional Challenges & Responses

The Covid-19 pandemic created unparalleled challenges for criminal justice authorities across the world. Lockdown measures forced courts in many countries to close to the public. Some of them managed to move trials online while others downscaled operations. Remote trials worked in some legal communities and for many types of hearing but not in every case. In major trials, both prosecution and defence experienced difficulties in presenting and examining live evidence online.

On the other hand, routine proceedings that required little interaction between the parties proved to be more efficient when held online. The pandemic prompted many judicial authorities to review their cyber security policies and upgrade digital technologies and implement more secure and efficient mechanisms for inter-agency collaboration and international cooperation.

The pandemic changed not just the delivery of justice but also the volume and typologies of crime. Vulnerabilities prompted by the pandemic have been widely exploited by criminals. Countries have reported surges in cybercrime, pandemic related fraud, and domestic violence. In response, prosecution authorities and the judiciary were prompted to adopt extraordinary strategies and novel policies to ensure business continuity.

This plenary session will explore how prosecution authorities responded to the pandemic. It will explore the extent to which the pandemic has accelerated prosecutorial innovations and performance, such as using Artificial Intelligence, and whether the one-time solutions deployed in response could become business as usual in the long-term. The session will discuss whether these transformations are sustainable and their impact on the efficiency and accessibility of criminal justice systems.

**The plenary session will include an interactive panel discussion and Q&A session.**



## WORKSHOP 1A

### Digital Transformation across Criminal Justice Systems

Over the last two decades private sector digital transformation has often outpaced public sector efforts. In criminal justice systems in particular, budgetary constraints, the conservative stance of criminal justice actors and many other factors have contributed to sluggish progress. The pandemic forced many criminal justice agencies to rethink and accelerate their approach to digital transformation.

During the pandemic, prosecution services and courts in many jurisdictions moved much of their businesses online to avoid a complete halt of proceedings. Other jurisdictions that had embarked on digital transformation before the pandemic further accelerated innovations.

As the pandemic recedes, it is worth exploring what pandemic-induced digital transformation worked (and what did not) and whether and how to make the changes sustainable and business as usual. The workshop participants will examine the factors behind the successes and failures and explore what lessons could be learned for the long-term digital transformation of different criminal justice systems.





There remains ample scope to make greater use of information technology in the sector. Artificial Intelligence, for example, has potential to automate highly routine processes and improve the overall quality of criminal justice services. The workshop will also provide a forum to showcase successful projects using Artificial Intelligence and other emerging technology.



## **WORKSHOP 1B**

### **Public Health Responses to Crime**

The global pandemic means that we are no longer able to rely on the outcomes and methods traditionally used in criminal justice systems. Substantial backlogs of cases are clogging up systems and already stretched resources are likely to reduce further as governments reduce their deficits. Out of necessity, people are looking for new ways of doing things. But this necessity and the current moment also provide an opportunity to rethink past practices and revisit the size, focus and operation of criminal justice systems.

There is a need to better understand the interrelationship between the public health of communities and the impact of justice systems and to develop strategies to address and prevent violence and other crime through a public health lens and without turning to carceral approaches as the first resort.

The workshop will explore best practices and models from around the world - in terms of both policy and operations - that emphasize public health rather than punitive solutions. It will examine how jurisdictions/prosecutors changed their approach in response to types of challenges that were exacerbated by the pandemic (such as domestic violence, behavioural and mental health issues) and how jurisdictions can ensure that the more promising solutions being put in place now are sustainable for the longer term, not just for the duration of the pandemic.





## PLENARY 2

### Evolution of Cybercrime Typologies

The world has undergone a dramatic digital transformation in the last couple of decades. At the same time cybercrime, from state sponsored cyber-attacks to low level fraud, has soared to new levels of prevalence and sophistication, phenomena accelerated by the pandemic. Rapidly emerging cybercrime typologies put an immense pressure on prosecution authorities, requiring constant changes in prosecution strategies, the updating of skills and the deployment of ever greater resources which are not always readily available.

At the same time, cooperation between criminal justice authorities and the private sector, particularly national and international service providers, is essential to understand cyber threats and the critical context of cybercriminal activities, to identify trends and facilitate the collection of digital evidence in cybercrime and other investigations and prosecutions.

Such cooperation not only allows access to data held by service providers, but also the sharing of experience, training, hardware, and software to assist authorities in cybercrime investigations and prosecutions. Arrangements between public authorities and the private sector often rely on a patchwork of agreements and would benefit from a more formalised framework for co-operation to help mitigate jurisdictional variations on data retention and sharing, conflicts concerning privacy issues and other common barriers to co-operation.

This session will explore the challenges related to the prosecution of established and emerging cybercrimes, including ransomware, phishing, violent extremism, and other crimes on the darknet, and the strategic and other responses of prosecution authorities. It will explore the roles of public-private partnerships and the use of Artificial Intelligence both by the perpetrators of cybercrimes and those tasked with the prevention and prosecution of their activity.

**The plenary session will include an interactive panel discussion and Q&A session.**



## WORKSHOP 2A

### Prosecuting Crimes on the Darknet

Darknet crimes are notoriously difficult to investigate and prosecute. Unsatisfactory criminal justice responses have contributed to a surge in cyber criminality in recent years, with perpetrators diversifying their criminal darknet activity and employing ever more sophisticated methods to avoid detection and investigation.

Beyond the growth and complexity of darknet crimes, there are many blurred lines in the laws regulating investigative techniques and practices that could be essential tools against darknet crimes. In this regard, rules governing the undercover operations on the cloud and remote searches are of note as such tools may accidentally or intentionally involve cross-jurisdictional activities by investigators.

In this very challenging environment, there are an increasing number of successful prosecutions of largescale darknet criminality. The workshop provides a forum for prosecutors and other criminal justice actors to present their cases and share their successful strategies.



## PLENARY 3

### Challenges of E-evidence across Borders

Criminal evidence is increasingly digital and, it follows, increasingly transnational. Fragmented and sometimes rigid rules of international law and divergent domestic laws and legal cultures can make transborder access to digital evidence challenging. Further, the legal boundaries between prohibited speech and freedom of expression vary across jurisdictions and has become increasingly controversial.

Digital evidence is inadmissible as evidence in some jurisdictions, while in others there are no clear rules or standards for its admissibility. To add to the complexity, the role of the private sector, particularly Internet Service Providers (ISPs) is critical to the preservation, retention and sharing of digital evidence.

Combined with a scarcity of appropriate but costly digital forensics and limited investigation and prosecution capacity, it is little surprise that cybercrime cases and other prosecutions relying on digital evidence often see significant delays or even fail.

The increasing complexity of emerging cybercrimes and the need to collect and properly process digital evidence across borders have prompted investigation and prosecution authorities to strengthen institutional capacities and introduce modern technologies. This session will explore the forensic capacity, resources, legislative and organizational solutions of prosecution authorities and the role of the private sector in the preservation and recovery of digital evidence. Further, it will examine the role of multi-lateral international actors in initiatives to promote cross-border access to digital evidence and the legal boundaries between prohibited speech and freedom of expression in the context of mutual legal assistance.

**The plenary session will include an interactive panel discussion and Q&A session.**



## WORKSHOP 3A

### Challenges of Obtaining Electronic Evidence from Abroad

This workshop will address challenges in the cross-border access to electronic evidence in the context of state-to-state as well as in public private cooperation. In recent decades, important international instruments have been introduced or initiated to assist with cross border access to electronic evidence. However, there are still largely divergent laws and procedural standards across jurisdictions that challenge practitioners in successful trans-border cooperation or direct access to electronic evidence.

Multinational online services providers hold an important key for the trans-border access to electronic evidence. While there are examples of good practice, not all of them are ready or willing to cooperate with foreign criminal justice authorities.

Prosecutors and other criminal justice actors will examine how the existing tools of cross-border access to electronic evidence work in practice. The workshop will explore how the newly designed and emerging international instruments will change the environment. The role of multinational





service providers will also be discussed alongside examples of successful and flawed cooperation with them.



## WORKSHOP 3B

### Freedom of Expression & Social Media

Internet based social networking sites (SNSs) have revolutionised modern communications. 1.62 billion users (a quarter of the world's population) visit Facebook alone each day. These developments obviously post-date the principal international human rights treaties that contain norms relating to freedom of expression. Moreover, the very nature of internet-based communications inevitably poses challenges for legal systems in terms of both applicable law and connection with territorially bounded jurisdictions.

For states, SNSs can represent an uncontrolled danger. For example, there was evidence that those involved in riots in the UK in 2011 had used SNS messaging to co-ordinate disturbances across London and other cities and elsewhere SNSs have been used to leak classified information harmful to national security. Many states have imposed 'Blocking' measures taken to prevent certain content from reaching an end-user. These include 'preventing users from accessing specific websites, Internet Protocol (IP) addresses, domain name extensions, the taking down of websites from the web server where they are hosted or using filtering technologies to exclude pages containing keywords or other specific content from appearing.

The potential implications on freedom of expression in relation to SNSs and other internet communications are most obvious when speech or expression is criminalised. The task for prosecutors in balancing the fundamental right of free speech and the need to prosecute serious wrongdoing often involves very difficult judgement calls.

The workshop will explore the tension that the application of an array of criminal legislation and jurisprudence in different jurisdictions has created with freedom of expression and whether the tension can be mitigated, and fundamental rights preserved.





## PLENARY 4

### Money Laundering through Virtual Assets

Identifying, assessing, and understanding money laundering (ML) risks by competent authorities are essential elements for the proper functioning of anti-money laundering systems. It assists with the prioritisation and efficient application of mitigation measures, including allocation of resources, commensurate with those risks.

Prosecutors are both contributors to and users of the risk assessment process. They may have relevant statistics on ML/TF investigations, prosecutions and convictions, assets seized, confiscated, repatriated, or shared or hold information about criminals' modus operandi obtained during an investigation. They may also be able to provide information on current trends and risks detected through their investigations and prosecutions as well as assist in identifying vulnerabilities.

Financial investigation can provide information about both proof of crime and property that may be subject to confiscation. Successful ML prosecutions, asset tracing, freezing and confiscation is extremely difficult without a prior financial investigation.

This session will examine the role of prosecutors in national ML risk identification, assessment, understanding and mitigation with a focus on virtual assets. It will examine the essential investigative techniques, strategies, and best practice for investigating, seizing, and confiscating virtual assets, including the use of domestic and international cooperation mechanisms, the use of multi-disciplinary/agency groups, FIU's, cooperation with regulators, and engagement with the private sector.

**The plenary session will include an interactive panel discussion and Q&A session.**



## WORKSHOP 4A

### Parallel Financial Investigations in Practice

Conducting parallel financial investigations regarding proceeds-generating crimes is both an international standard and a trend that is pursued in practice. However, doing it routinely and effectively remains a challenge. The workshop will investigate the approaches promoted by the international standards and practices employed by different countries for overcoming the challenges and achieving the high quality and routine application of parallel financial investigations.



## WORKSHOP 4B

### Tracing, Seizing & Freezing Virtual Assets

The workshop will be based on case studies of the tracing, freezing and confiscation of virtual assets. The case studies will demonstrate the importance of financial investigations, the legal and practical challenges of recovering virtual assets and how those challenges were overcome.