Privanova
Research & Consulting

UN CONVENTION ON COUNTERING THE USE OF ICTS FOR CRIMINAL PURPOSES

Privanova's contribution to the Reconvened Concluding Session of the Ad Hoc Committee

New York, July 29 - August 9, 2024

CONTACT

privanova.com

contact@privanova.com

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

Acknowledgments

We would like to express our sincere gratitude to several individuals and organisations whose support and contributions were invaluable in the preparation and presentation of this position paper at the Reconvened Concluding Session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes.

First and foremost, we thank the United Nations Office on Drugs and Crime (UNODC) for organising this significant event and providing a platform for discussion and collaboration on such a critical issue. We appreciate the efforts of the Ad Hoc Committee, and the Consistency Group for their dedication and hard work in drafting and refining the convention.

We also acknowledge the support of our colleagues at Privanova, whose expertise and commitment were instrumental in the development of this paper. Their collaborative spirit and dedication to advancing cybersecurity and privacy have been truly inspiring.

Lastly, we extend our appreciation to our partners in various EU-funded projects that have contributed to our expertise and understanding of cybersecurity, privacy, and related fields. These projects include GeoFlexHeat (GA 101096799), ELOQUENCE (GA 101070558), CONVERT (GA 101070076), SECUR-EU (GA 101070009), IMERMAID (GA 101070187), POLIIICE (GA 101070029), DRG4FOOD (GA 101060660), GLOCALFLEX (GA 101069673), FACILITATE (GA 101070047), CYBERSPACE (GA 101070557), TRACE (GA 101070183), and DigiCare4You (GA 945246). The collaborative efforts and knowledge gained through these initiatives have been instrumental in shaping our perspectives and recommendations presented in this position paper.

Introduction

Privanova, a pioneering research and development consultancy, operates at the intersection of privacy, technology, and policy. Specialising in the examination of legal, technological, ethical, and policy-related issues within the field of cybercrime, we offer a unique perspective grounded in the expertise of our team, which includes former professionals from the UN, INTERPOL, and the EU who have been involved in large-scale, interdisciplinary research projects.

Our contribution to the Reconvened Concluding Session of the UN's Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes builds upon our active participation in all prior Intersessional Consultations. The document we present today addresses the key issues scheduled for discussion during this final session, including international cooperation, provision of technical assistance, cybercrime prevention measures, and the practical aspects of implementing these strategies.

Our aim is to provide a comprehensive and practical perspective on these issues, informed by our unique experiences and the innovative approaches we have developed through our wide-ranging, interdisciplinary research projects. We trust that our insights will make a valuable contribution to the ongoing discourse surrounding the use of information and communication technologies for criminal purposes.

Recommendations

As a leading research and development consultancy at the forefront of privacy, technology, and policy, we present a set of recommendations aimed at addressing some of the most pressing issues in the fight against cybercrime. Our ambition is to provide a comprehensive and practical perspective on these issues, fuelled by our unique experiences and innovative approaches developed within our wide-ranging, interdisciplinary research projects. Our recommendations focus on the following key areas:

Strengthening Human Rights Safeguards

The integration of specific human rights safeguards throughout the entire treaty is paramount. Ensuring compliance with principles of legality, necessity, proportionality, non-discrimination, and legitimate purpose is critical. We recommend adding explicit references to key human rights affected by the Convention, such as privacy, fair trial, and non-discrimination.

Enhancing Data Protection

Detailed data protection safeguards must be included in the convention to ensure clear, precise, and unambiguous standards for personal data transfer. Transparency and accountability in data sharing are essential, and mechanisms for individuals to challenge problematic requests should be established.

Improving Procedural Measures and Law Enforcement

We advocate for requiring independent judicial authorisation for surveillance and ensuring adequate notification of individuals once it no longer jeopardises investigations.

Fostering Interoperability of Cybercrime Prevention and Detection Platforms

The escalating complexity and frequency of cybercrime necessitate a coordinated and collaborative international response. We recommend that the UN Ad Hoc Committee focus on fostering the interoperability of cybercrime prevention and detection platforms, building on the existing work and knowledge shared within our cluster. Establishing global standards or protocols to ensure compatibility and seamless interaction between different platforms is vital. For example, the CYBERSPACE project, funded by the EU through the Horizon 2020 program, has demonstrated the significance of interoperable systems by improving cyberattack reporting mechanisms and collaboration efforts among law enforcement agencies.

Establishing a Unified System for Reporting Cybercrimes

A consistent and globally unified approach to cybercrime reporting is essential. We recommend the establishment of a standardised, accessible, and globally unified system for reporting cybercrimes. Such a system should encourage victims to report incidents, leading to improved data collection and more effective strategies to combat cybercrime while ensuring the privacy and safety of individuals.

Fostering Global Cooperation and Effective Response

By focusing on interoperability and unified reporting systems, the UN Ad Hoc Committee can foster global cooperation and effectively respond to the challenges posed by cybercrime. This approach will aid in the optimal use of resources, knowledge, and expertise across countries, thus enhancing our collective ability to counter cyber threats.

Promoting Collaborative Research and Shared Learning

Under Privanova's leadership, the EU Commission project promotes shared learning and collaborative research across various sectors, including academia, industry, law enforcement, and policy-making. This interdisciplinary dialogue leads to practical, well-rounded solutions that address the pressing challenges of cybercrime. Our contribution builds upon our participation in all previous Intersessional Consultations and reflects our ongoing commitment to advancing cybersecurity collaboration.

Narrowing the Scope of the Convention

One of our primary recommendations is to narrow the scope of the Convention to clearly defined, existing cyber-dependent crimes. This approach ensures legal certainty and foreseeability while minimising potential abuse. Limiting the scope of procedural measures to the investigation of criminal offences set out in the Convention is crucial for maintaining focus and effectiveness.

Conclusion

In conclusion, the fight against cybercrime demands a comprehensive, collaborative, and human rights-centric approach. Our recommendations emphasize the critical need for robust safeguards to protect fundamental rights and enhance data protection throughout the Convention. We advocate for improved procedural measures in law enforcement, ensuring transparency and accountability in surveillance activities.

The interoperability of cybercrime prevention and detection platforms, coupled with a unified global reporting system, stands as a cornerstone for effective international cooperation. These measures will significantly enhance our collective ability to combat cyber threats and respond swiftly to emerging challenges.

Furthermore, we stress the importance of promoting collaborative research and shared learning across sectors, fostering an environment of continuous improvement and innovation in cybersecurity. By narrowing the Convention's scope to clearly defined cyber-dependent crimes, we aim to ensure legal certainty and focused, effective action against cybercrime.

As we stand at this critical juncture, the international community has a unique opportunity to forge a path towards a safer digital future. By adopting these recommendations, we can create a robust framework that not only addresses the complex challenges of cybercrime but also upholds the values of human rights, privacy, and global cooperation. Together, we can build a digital world that is secure, resilient, and respectful of individual freedoms – a world where technology empowers rather than endangers, and where international collaboration triumphs over cybercrime.

Privanova

Research & Consulting