Cybercrime Digest

Bi-weekly update and global outlook by the
Cybercrime Programme Office of the Council of Europe (C-PROC)

1-15 May 2018

Source: Council of Europe

Date: 15 May 2018

Global state of cybercrime legislation reviewed

"The "global state of cybercrime legislation" was reviewed today in a workshop organised by the Council of Europe at the UN Crime Commission in Vienna. Between 2013 and 2018 good progress was made worldwide in terms of criminalisation. About half of UN member States now have substantive laws in place largely in line with the Budapest Convention on Cybercrime. Limited progress was made regarding procedural law. Speakers pointed at the risk that vague provisions in cybercrime laws may be used to prosecute free speech and that investigated powers are not always limited by conditions and safeguards as required by the Budapest Convention. The event was held in partnership with the Governments of Argentina, Portugal, Romania, Sri Lanka and United Kingdom as well as the European Union." READ MORE

Source: World Trademark Review

Date: 14 May 2018

ICANN releases new WHOIS specification plan as GDPR countdown nears zero

"ICANN has published its Temporary Specification for gTLD Registration Data in a bid to ensure WHOIS compliance with the European Union's General Data Protection Regulation (GDPR), while maintaining the existing WHOIS system to the greatest extent possible. Subject to further revision prior to a board vote, the model proposes the establishment of a mechanism to allow contact with domain name registrants – while cloaking their identity. As we have reported previously, last month the Article 29 Data Protection Working Party (WP29) responded to ICANN's initial request for feedback on a proposed interim model for ensuring that the treatment of WHOIS data is compliant with GDPR. While welcoming the decision of ICANN to propose an interim model which involves layered access, the WP29 raised a number of concerns. With the May 25 enforcement date for GDPR two weeks away, the past few days have seen a flurry of activity at ICANN HQ." READ MORE

RELATED ARTICLES

Domain Name Wire, Google has already GDPR'd its Whois records, 7 May 2018

Source: ZD Net

Date: 14 May 2018

Cyber crime: Under-reporting of attacks gives hackers a green light, say NCA UK

"Organisations which don't report that they've been the victim of cyber crime are putting others at risk of further attacks and are hampering the authorities' ability to fight against hackers, the UK's serious and organised crime unit has warned. The National Crime Agency has issued the warning to businesses as part of its National Strategic Assessment of Serious and Organised Crime 2018. "Under-reporting of data breaches continues to erode our ability to make robust assessment of the scale and cost of network intrusions," said the report, adding "many companies are not disclosing data breaches, putting victims at risk". […] The Assessment suggests that the lack of successful cyber crime reporting means that cyber attackers believe that there's no consequences of their actions." READ MORE

Source: Europol

Date: 8 May 2018

Eight arrested for distribution of child sexual abuse material through Skype and the darknet

"Europol has supported the Spanish National Police on Operation Sky, a complex investigation targeting the distribution of child sexual exploitation material through darknet platforms and Skype. The investigation led by the Spanish National Police's High-Tech Crime Unit began in mid-2017 and focused at first on the TOR network. Prompted by clear evidence of the prolific sharing of indecent images, the Spanish investigators uncovered links diverting users to a private group accessible by invitation only on Skype. […] The group members from 14 different countries were actively exchanging child sexual abuse and exploitation material. Operation SKY aimed at clearly identifying, charging and prosecuting them for encouraging child sexual exploitation and abuse through their activities. The investigators monitored the activity online using innovative operational resources in this complex case. They also dealt with the demands of different legal frameworks in a worldwide investigation. The house searches and arrests followed shortly after." READ MORE

Source: SC Magazine

Date: 8 May 2018

Cybercrime losses in U.S. exceed $1.4B in 2017

"Losses of cybercrime victims exceeded $1.4 billion in 2017, according to the latest FBI 2017 Internet Crime report. The top three cybercrimes reported by victims in 2017 were non-payment/non-delivery crimes with 84,079 victims, personal data breaches with 30,904 victims, and phishing with 25,344 victims. Two of the top three crimes, non-payment/non-delivery, and personal data breaches were also in the top spot in 2016 while phishing beat out 419/overpayment scams which dropped to fourth place in 2017, affecting only 23,135 victims compared to the 25,716 victims in 2016. The report's data represents a total of 301,580 complaints filed with the Internet Complaint Center (IC3) in 2017 alone. The goal of the report is to increase public awareness about current internet scams and fraud as the Bureau encourages users to report any cybercrimes they may witness." READ MORE

Source: Infobae

Date: 13 May 2018

Argentina se suma a la Convención de Budapest para tratar delitos informáticos

"En noviembre de 2017, la Cámara de Diputados aprobó la ley de ratificación de la Convención de Budapest, un tratado internacional de más de 56 países en la búsqueda de cooperación para la lucha contra delitos informáticos. Con la firma del presidente Mauricio Macri, la semana pasada, la Argentina ya está oficialmente adentro de la Convención (solo restan pasos burocráticos). […] El abogado Marcos Salt, coordinador académico del Programa Nacional Contra la Criminalidad Informática del Ministerio de Justicia, explica a Infobae: "Argentina comenzó a analizar la Convención de Budapest, con idas y vueltas, pero siempre con un tono muy favorable. En último cambio de gobierno, he retomado la idea de unirnos a la Convención. […] El objetivo principal del Convenio de Budapest es la cooperación entre los Estados de los países que lo integran y el sector privado. El tratado tiene 4 capítulos y propone la integración (u homogeneización) de normas procesales e investigación cooperativa de conductas ilegales en internet. Uno de los requisitos para entrar al Convenio es la modernización de la ley procesal. "Argentina tiene la ley penal bien para sumarse a la Convención. Pero vamos a tener que modificar algunas normas procesales." READ MORE

Source: PTV

Date: 13 May 2018

Philippines, Department of Justice holds cybercrime training for judges in Cebu

"The Department of Justice – Office of Cybercrime (DOJ-OOC) has conducted an Introductory Training on Cybercrime and Electronic Evidence for Judges, in partnership with the Supreme Court and Global Action on Cybercrime Extended (GLACY+) Project. The three-day training, held from May 8 to 10, in Cebu provided cybercrime court judges with the current landscape in handling cybercrime and cyber-related cases, including varied discussions on jurisdiction and electronic evidence. Various experts from the judiciary and the DOJ served as resource speakers and facilitators on topics pertaining to Cybercrime Law, the Budapest Convention on Cybercrime, electronic evidence, and digital forensics, among others. The training was attended by more than 60 Judges assigned outside the National Capital Judicial Region (NCJR)." READ MORE

Source: APA News

Date: 3 May 2018

Gambia pushes for legislation to combat cyber-crime

"The Gambia government has embraced a global advisory mission backed by the European Union (EU) and the Council of Europe for the establishment of legislative measures needed for the investigation of cyber-related crimes. The desire for legal provisions on cyber-crime and electronic evidence in a court of law was acknowledged by stakeholders in the ICT, security and legal sectors at the opening of a three-day capacity building workshop on cyber-crime. It got under way on Wednesday at a local hotel in Banjul, and the training course is being executed by cyber-crime experts from Europe, within the framework of the Global Action on Cyber Crime Extended (GLACY+) Joint project of the EU. Gambia's Minister of Information and Communication Infrastructure, Demba Ali Jawo, speaking at the event outlined the government's position in the fight against cyber-crime." READ MORE

Source: 20 Minutos

Date: 7 May 2018

Mexico, Policía Federal atendió más de 233 mil incidentes cibernéticos

"Durante cinco años de la presente administración, la Policía Federal (PF) ha identificado más de 233 mil incidentes cibernéticos en el país, informó el director general del Centro Especializado en Respuesta Tecnológica, Radamés Hernández Alemán. "Es una cantidad que sí representa un gran volumen para nuestro país, más de 60 por ciento de incidentes tiene que ver con infección por códigos maliciosos, lo cual nos quiere decir que mucha de las afectaciones se están realizando con uso de la tecnología", explicó." READ MORE

Source: All Africa

Date: 14 May 2018

Hurdles in Combating Cybercrime in Nigeria

"The Executive Chairman/Chief Executive Officer, Nigeria Communication Commission (NCC), Prof. Umar Garba Danbatta has pointed out various challenges involved in the fight against cybercrime in Nigeria. He said the absence of comprehensive and reliable demographic and database; insufficient expertise in the area of Cyber and information security; insufficient inter agency, regional and international collaboration and lack of effective and functional forensics labs, technics and manpower to match the speed, anonymity and fleeting nature of evidence in cybercrimes investigation are the numerous challenges encountered in cybercrime management in Nigeria." READ MORE

Source: Eurojust

Date: 4 May 2018

The European Judicial Cybercrime Network meets at Eurojust to discuss e-evidence initiatives

"On 25 and 26 April 2018, the fourth plenary meeting of the European Judicial Cybercrime Network (EJCN) took place at Eurojust. […] Special attention was given to the proposals published 17 April 2018 on the Regulation on European Production and Preservation Orders for electronic evidence in criminal matters and the Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings. Additionally, recent legislation and other initiatives on e-evidence such as the US CLOUD Act, the Second Additional Protocol to the Budapest Convention and the Sirius platform to facilitate online investigations were discussed." READ MORE

Source: France Diplomatie

Date: 2 May 2018

Vision commune du président de la République française et du premier ministre d'Australie sur la relation franco-australienne

"41. […] L'Internet est de plus en plus utilisé à des fins malveillantes par des terroristes, des pédophiles et des groupes criminels. Comme convenu lors du G20 de 2017, les lois en vigueur hors ligne devraient également s'appliquer en ligne. Nous sommes attachés à garantir l'existence de cadres visant à préserver la sécurité des populations tout en faisant respecter les droits et les libertés fondamentales. À cet égard, les dirigeants ont réitéré leur attachement commun à la Convention de Budapest sur la cybercriminalité." READ MORE

Source: Loop Tonga

Date: 15 May 2018

Regional cyber security workshop opens in Tonga

"Tonga Prime Minister 'Akilisi Pohiva opened a regional cyber security workshop in Tonga on 14 May. […] He stated that the Government of Tonga has made various steps to assist in creating resilience to cyber threats such as the establishment of the cyber challenges taskforce in 2013 and Tonga CERT and its board in 2016 and Tonga acceding to the Budapest Convention on Cybercrime last year. […] Acting Australian High Commissioner, Ms. Rhona McPhee said that Cyber Cooperation is something that Australia takes very seriously, and is working closely with the Pacific Island Countries. "Here in Tonga, we acknowledge the proactive efforts of the Government to improve cyber security systems and legal frameworks, the first Pacific Island country to accede to the Budapest Convention." Australia's first International Cyber Engagement Strategy was launched by the Foreign Minister in October 2017 priorities and coordinates a whole-of-Government approach to international engagement across the full spectrum of cyber affairs. […] "The Cyber Capacity Building element of the Strategy is support by the Cyber Cooperation Program, $14 million over four years, 2016-2020."" READ MORE

Source: Kaieteur News

Date: 8 May 2018

Guyana recommended to replace Cybercrime Bill

"Attorney-at-Law, Christopher Ram has recommended that Government produce a new Cybercrime Bill to the National Assembly that conforms to the internationally-accepted Budapest Convention. […] The Organisation of American States through its ministerial working Group on cybercrime has been steering members towards the adoption of the Convention." READ MORE

Source: KBC

Date: 14 May 2018

Computer and Cybercrime bill awaits Presidential assent in Kenya

"The Computer and Cybercrime bill 2017 that awaits Presidential ascent has prescribed hefty penalties for hackers who gain unauthorized access to computers or data of institutions, individuals or government. In recent years, various state agencies, financial institutions have suffered massive losses as a result of data breach. Last month IT services firm Serianu released its annual cybercrime report indicating that in Kenyan lost KES 21.2B to cybercriminals. It is expected that the new bill will discourage hacking, identity theft, and spread of malicious malware. […] The bill also stipulates stiff penalties on cyber espionage, false publications, child pornography, computer forgery cyberstalking and cyber-bulling." READ MORE

Source: ITP.net

Date: 2 May 2018

Dubai Police launch public cybercrime reporting website

"Major General Abdullah Khalifa Al Marri, Commander-in-Chief of Dubai Police, has launched the eCRIME online platform to receive reports of cyber crimes from members of the public. The website - www.ecrime.ae - has been launched in accordance with the Dubai 2021 Plan and allows internet users to report any suspicious online activity. Al Marri stressed the keenness of the Dubai Police on providing innovative services in line with the strategic directions of the UAE and the future plans of the Government of Dubai in the field of smart services." READ MORE

Source: Tribune 242

Date: 11 May 2018

Bahamas, 80 Percent Increase In Cyber Crime

"CYBER crime in the Bahamas showed an 80 percent increase, with 171 incidents reported in 2017 up from the 95 recorded in 2016. […] Currently there are separate pieces of legislation that govern cyber security, the minister said. "The Computer Misuse Act (CMA) which was instituted in 2003 -- this Act provides comprehensive criminalisation of and procedural law for cyber criminal activity in the country," he said. "Parliament also signed the Data Protection Act (2003) and the Electronic Communication & Transactions Act (2006)." Both laws, Minister Dames said safeguards the rights of citizens online and establishes norms and regulations for e-commerce and other online services." READ MORE

Source: Fiji Sun Online

Date: 4 May 2018

Fiji urged to amend cybercrime legislation

"The Citizens' Constitutional Forum (CCF) has recommended that an amendment be made to the Crimes Act of 2009 to incorporate regulations to govern communication through all electronics devices which can access the internet. CCF Representative and lawyer Lusia Lagilevu while making submissions to the Standing Committee on Justice, Law and Human Rights yesterday stated there was existing legislation that addresses some aspects of Cyber Crime and related issues. She said the Crimes Act addresses Cyber-crimes though the offences substantially only involved the use of computers in Division 6 of the Act. […] She highlighted that during his speech at last year's Attorney-General's Conference, the Police Commissioner Brigadier-General Sitiveni Qiliho stated that the Crimes Act was silent on digital devices like mobile phones, tablets that also can store and disseminate data." READ MORE

Latest reports

- Council of Europe, Cybercrime: the state of legislation, 15 May 2018
- FBI, Internet Crimes Report 2017, May 2018
- UK, National Crime Agency, National Strategic Assessment of Serious and Organized Crimes, May 2018
- Portugal, Centro de Estudos Judiciarios, O dominio do imaterial: Prova digital, Cibercrime e a Tutela Penal de Direitos Intelectuais, May 2018

Upcoming events

- 14-18 May, Vienna, Austria – Participation in the UN Commission on Crime Prevention and Criminal Justice, Cybercrime@EAP 2018 / GLACY+ / iPROCEEDS / CyberSouth / Cybercrime@Octopus
- 17-18 May, Podgorica, Montenegro – Pilot training session on introductory training courses on cybercrime, e-evidence and online crime proceeds for judges and prosecutors (2nd part), iPROCEEDS
- 21-24 May, San Jose, Costa Rica – Initial Assessment Visit and establishment of the National Team, GLACY+
- 21-24 May, Turkey – Case simulation exercise on cybercrime and financial investigations, iPROCEEDS
- 22-24 May, Minsk, Belarus – Workshop on Cybercrime Threats, Strategies and Online Resource, Cybercrime@EAP 2018
- 28-29 May, Port Louis, Mauritius – Advisory mission on cybercrime reporting and workshop on collection and monitoring of criminal justice statistics on cybercrime and electronic evidence, GLACY+
- 28 May - 1 June, Santo Domingo, Dominican Republic, ECTEG Course: Live-Data Forensics for law enforcement officers, GLACY+
- 30-31 May, Tirana, Albania – Pilot introductory training course on cybercrime, electronic evidence and online crime proceeds for judges and prosecutors (1st part), iPROCEEDS
- 31 May, Turkey – Advice on lessons learnt from case simulation exercises, iPROCEEDS
- 31 May, C-PROC – Analysis of the project of Cybercrime bill in Brazil, GLACY+

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

www.coe.int/cybercrime