Cybercrime Digest

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

1-15 April 2019

Source: U.S. Department of Justice

Date: 10 Apr 2019

U.S. Justice Department Announces Publication of White Paper on the CLOUD Act

"The Department announced today the public release of a white paper on the Clarifying Lawful Overseas Use of Data Act, known as the CLOUD Act. The CLOUD Act was enacted in March 2018 and updates the legal framework for how law enforcement authorities may request electronic evidence needed to protect public safety from service providers while respecting privacy interests and foreign sovereignty. […] The CLOUD Act has two distinct parts. First, the Act authorizes the United States to enter into bilateral agreements to facilitate the ability of trusted foreign partners to get the electronic evidence they need to combat serious crimes. In order to qualify under the Act, a partner country must adhere to baseline rule-of-law, privacy, and civil liberties protections. […] Second, the CLOUD Act makes explicit in U.S. law the established principle – longstanding in both the United States and in many foreign countries – that a company subject to our jurisdiction can be required to produce data within its custody and control, regardless of where it chooses to store that data at any point in time." READ MORE

RELATED ARTICLES

U.S. Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, White Paper, April 2019

Source: Eurojust

Date: 5 Apr 2019

The European Union takes a stand against cybercrime

"Judicial practitioners from across Europe gathered at Eurojust, the EU's Judicial Cooperation Unit, for the 6th European Judicial Cybercrime Network (EJCN) plenary meeting, to strengthen the fight against ever-evolving threats posed by cybercrime. The EJCN provides a cross-border platform to exchange national experience and best practice, get inspiration from other legal systems, discuss real case examples, and find practical solutions in countering cybercrime. It explores the boundaries of the existing legal frameworks in the Member States and works to best interpret these systems to step up the investigation and prosecution of cybercriminals and produce evidence that can hold up in court." READ MORE

Source: Matinal

Date: 9 Apr 2019

Bénin, les acteurs de droit s'approprient la Convention de Budapest

"L'Agence nationale de la sécurité des systèmes d'information (Anssi), en collaboration avec le ministère de l'Economie numérique et de la communication a organisé, le vendredi 5 avril 2019, un atelier d'information sur la Convention de Budapest sur la cybercriminalité. Cet atelier entre dans le cadre de l'harmonisation régionale des lois, en conformité avec les normes internationales, vers une coopération contre la cybercriminalité. Les magistrats, les officiers de policeet les ingénieurs s'approprient la Convention de Budapest sur la cybercriminalité. Le but de cet atelier est de s'informer sur cet arsenal juridique international pour une adhésion du Bénin." READ MORE

Source: Ghana Justice

Date: 13 Apr 2019

Ghana, Parliament ratifies Convention on cybercrime

"Parliament has ratified the Convention on Cyber Crime (Budapest Convention) after the report of the Parliamentary Select Committee on Communication was presented at the Plenary. The report was presented by the Chairman of the Communications Committee and Member of Parliament, Mr. Kennedy Ohene Agyapong. […] Mr. Agyapong explained that an assessment conducted by the World Bank and the Global Cyber Security Capacity Centre of Oxford University on Ghana, revealed that one major obstacle to fighting cybercrime was the lack of an effective international cooperation framework for investigations and prosecutions. […] Mr. Agyapong indicated that the objective of the Convention seeks to facilitate international co-operation on prevention, investigations and prosecution of cybercrimes." READ MORE

Source: Sapo Notìcias

Date: 11 Apr 2019

Comunidade dos Países de Língua Portuguesa (CPLP): estratégia comum para combate ao Cibercrime

"Pedro Vedelho que é quadro da Procuradoria-Geral de Portugal, se encontra na Cidade da Praia para participar da conferência internacional sobre o Cibercrime e na 2ª reunião do Fórum Cibercrime, organizado pelo Fórum que tem a sua sede em Lisboa e pela Procuradoria-Geral da República de Cabo Verde. Segundo explicou, com a criação desse fórum que é uma rede de ponto de contactos dos magistrados de todos os países da CPLP, pretende-se estabelecer a troca de experiência e de opiniões, análises legislativas sobre cirbercrime e a obtenção da prova digital. […] O coordenador do fórum Cibercrime lembrou que vários países integrantes da comunidade já têm uma lei do cibercrime "bastante estruturada e parecida", o que facilita a investigação e a cooperação, sendo certo que a aposta deve ser no reforço da cooperação internacional dado à sua complexidade e a natureza. A adesão à Convenção de Budapeste é para já importante. Portugal e Cabo Verde já aderiram e outros países já deram algum passo e há outros que estão a ponderar. Neste sentido o encontro da Praia servirá também para sensibilizar os outros a aderirem a esta convecção." READ MORE

RELATED ARTICLES

Sapo Notìcias, Conselho de Europa pede adesão de países lusófonos a convenção sobre cibercrime. Apenas Portugal e Cabo Verde integram, 11 Apr 2019

Source: Guinee News

Date: 3 Apr 2019

Cybercriminalité: la Guinée vers une adhésion à la convention de Budapest

"Après avoir ratifié la convention de Malabo sur la cybercriminalité en 2017, la Guinée projette d'adhérer à la convention de Budapest qui prône la cybersécurité et la protection des données à caractère personnel. Ce mardi 2 avril, un atelier d'information sur ladite convention, a été organisé à Conakry par le Conseil de l'Europe en collaboration avec le ministère des Télécommunications et de l'Economie Numérique. Cette rencontre qui a été présidée par le ministre des Télécommunications Moustapha Mamy Diaby, a connu la présence du Secrétaire exécutif de la Convention de Budapest sur la criminalité, du Directeur central de la police judiciaire, du président de la commission des Télécommunications de l'Assemblée Nationale, des cadres des départements des Postes et Télécommunications, de la Sécurité, de la Justice ainsi que des officiers de la gendarmerie et de la police nationale." READ MORE

Source: UK Government

Date: 8 Apr 2019

UK, Open Consultation on the On-Line Harms White Paper

"The Online Harms White Paper sets out the government's plans for a world-leading package of online safety measures that also support innovation and a thriving digital economy. This package comprises legislative and non-legislative measures and will make companies more responsible for their users' safety online, especially children and other vulnerable groups. The White Paper proposes establishing in law a new duty of care towards users, which will be overseen by an independent regulator. Companies will be held to account for tackling a comprehensive set of online harms, ranging from illegal activity and content to behaviours which are harmful but not necessarily illegal. This consultation aims to gather views on various aspects of the government's plans for regulation and tackling online harms" READ MORE

Source: ZD Net

Date: 3 Apr 2019

Over 540 million Facebook records found on exposed cloud servers

"Data breach hunters have found two Amazon cloud servers storing over 540 million Facebook-related records that have been collected by two third-party companies. The number of affected users is believed to be in the range of millions and tens of millions. Both servers have been discovered earlier this year by security researchers from UpGuard, a California-based cyber-security firm specialized in identifying data leaks. The first server contained most of the data, and belonged to Cultura Colectiva, a Mexico-based online media platform operating across Spanish-speaking Latin America countries. At a size of 146GB, this AWS server stored over 540 million records detailing user account names, Facebook IDs, comments, likes, reactions, and other data used for analyzing social media feeds and user interactions. The second AWS server stored data recorded by the "At the Pool" Facebook game. This included details such as the Facebook user ID, a list of Facebook friends, likes, photos, groups, checkins, and user preferences like movies, music, books, interests, and other, along with 22,000 passwords." READ MORE

Source: BBC

Date: 4 Apr 2019

Concern over Singapore's anti-fake news law

"This week Singapore's government proposed its anti-fake news law in parliament - the Protection from Online Falsehoods and Manipulation Bill. The government says the law is necessary to protect Singaporeans from fake news and educate them about potential damage it can cause - in particular inciting racial and religious disharmony. But critics say this new law puts too much power in the hands of the Singapore government, potentially threatening civil liberties. Under the new law Singapore's government will determine what is factual news and what is not. If there is content about public institutions the government says is false, it can issue corrections that must be published, though it is yet unclear the exact process of how that would happen. In extreme cases, it can tell online platforms to remove content it deems false. This would affect not just individuals but also social media sites like Facebook, Google and Twitter which have their regional headquarters in Singapore." READ MORE

RELATED ARTICLES

The Economist, Asian governments are trying to curb fake news, 4 April 2019

Source: Global Banking and Finance Review

Date: 3 Apr 2019

APWG.EU Cyber Security Awareness Symposium examines behavioral interventions against cybercrime at global scale

"APWG.EU is holding its fourth annual Symposium on Global Cybersecurity Awareness in partnership with the European Commission and the Council of Europe (Convention on Cybercrime) on June 26-27, to be held at the European Commission Representation Office in Bucharest with the theme of Considering Behavioral Interventions at Global Scale. The objectives of the Symposium, inaugurated by APWG.EU in 2016, are the establishment of global strategies for cybersecurity awareness development " and the cultivation of research, measurement tools and awareness assets deployed as instruments of cybercrime prevention regimens, subject to the same rigor as any other kind of public health measure." READ MORE

Source: El Comercio

Date: 15 Apr 2019

Al Ministerio del Interior le preocupa la legislación, tecnología y personal para enfrentar ciberataques en Ecuador

"Estamos tomando las alertas". María Paula Romo, ministra del Interior, señaló que el retiro del asilo a Julian Assange, quien el jueves 11 de abril del 2019 fue sacado por la Policía de la Embajada de Ecuador en Londres, tiene un impacto en ataques a portales digitales. Romo llegó la mañana de este lunes 15 de abril del 2019 a Cuenca para una ceremonia en la que se oficializó la llegada de 187 nuevos policías para reforzar la seguridad en la provincia del Azuay. En ese marco, la ministra dijo que le preocupa que el Ecuador es uno de los pocos países de la región que no cuenta con una ley para luchar contra ciberdelitos, con tecnología y personal. De hecho, la Ministra enfatizó que el país no ha firmado ni ratificado el Convenio sobre Ciberdelincuencia, vigente desde el 1 de julio del 2004, con países de Europa, además de Canadá, Japón, Estados Unidos, Sudáfrica, Panamá, Perú, entre otros. Dicho instrumento, también llamado Convenio de Budapest, es el primer tratado internacional que busca armonizar leyes nacionales, desarrollar técnicas de investigación y fortalecer la cooperación entre naciones para hacer frente a los delitos informáticos y los delitos en Internet." READ MORE

RELATED ARTICLES

AFP, Ecuador Says Hit by 40 Million Cyber Attacks Since Assange Arrest, 15 Apr 2019

Source: National Crime Agency UK

Date: 12 Apr 2019

UK student behind $100m dark web site jailed for 5 years 4 months

"An unemployed university drop-out has been jailed for five years four months years after running a dark web business selling illegal drugs and for hoarding a catalogue of horrific child sex abuse images. Thomas White, 24, took over the running of the notorious dark web site Silk Road after it the FBI closed it in 2013. White, who left his accounting degree at Liverpool John Moores University after a single term, was an administrator of the Silk Road. But within a month of its shutdown he launched Silk Road 2.0. Like the original site, it used technology to allow users to anonymously buy and sell drugs, computer hacking tools and other illegal goods, using the digital currency bitcoin." READ MORE

Source: KrebsOnSecurity

Date: 8 Apr 2019

A Year Later, Cybercrime Groups Still Rampant on Facebook

"Almost exactly one year ago, KrebsOnSecurity reported that a mere two hours of searching revealed more than 100 Facebook groups with some 300,000 members openly advertising services to support all types of cybercrime, including spam, credit card fraud and identity theft. Facebook responded by deleting those groups. Last week, a similar analysis led to the takedown of 74 cybercrime groups operating openly on Facebook with more than 385,000 members." READ MORE

Source: AFP

Date: 8 Apr 2019

Leap in Cyber Attacks Against Elections in OECD Countries

"Cyber attackers targeted half the member states of the Organization for Economic Cooperation and Development (OECD) that held national elections in 2018, the agency that monitors Canada's telecoms networks said Monday. "The proportion of elections targeted by cyber threat activity has more than tripled" since 2015, said the Canadian Security Establishment (CSE), which warned of a further spike this year. […] The report said voters were now the target of cyber activity rather than political parties, candidates or their staff, accounting for more than half of global activity in 2018. […] The goal of the cyber attackers was to "manipulate online information... in order to influence voters' opinions and behaviors," the report said." READ MORE

Source: South China Morning Post

Date: 4 Apr 2019

Hong Kong's top court rules against use of 'one-size-fits-all' charge for smartphone crimes

"Charge of 'obtaining access to computer for criminal or dishonest gain' should not apply to person's own devices, court says. […] Hong Kong's top court has struck down the use of a "one-size-fits-all" charge often used in the prosecution of smartphone-related crimes, including the taking of upskirt photos and videos, opening legal loopholes that will make law enforcement difficult. The landmark decision on Thursday meant the Department of Justice would have to re-evaluate 13 cases currently on hold, while facing possible appeals from those already convicted. Legal experts already raised concerns that other available charges would not be sufficient to plug the loopholes and new legislation would be needed. In Thursday's ruling, the Court of Final Appeal unanimously dismissed the justice secretary's appeal, upholding a lower court's decision and finding that the charge of "obtaining access to a computer for criminal or dishonest gain" should not apply to a person's own phone or computer." READ MORE

Latest reports

- European Commission, Ethics guidelines for trustworthy AI, 8 Apr 2019
- G7, Foreign Ministers Meeting Communiqué, 5-6 Apr 2019
- European Data Protection Supervisor, EDPS Opinion regarding the participation in the negotiations in view of a Second Additional Protocol to the Budapest Cybercrime Convention, 2 Apr 2019
- EU Cyber Direct, European Cyber Diplomacy Dialogue – Opening Lecture, posted on 9 April 2019
- Symantec, Two in Three Hotel Websites Leak Guest Booking Details, 9 Apr 2019
- Tactical Tech, Personal Data: Political Persuasion – Inside the Influence Industry, March 2019

Upcoming events

- 22 – 25 April, Bosnia and Herzegovina – Introductory training course on cybercrime, electronic evidence and online crime proceeds for judges and prosecutors, iPROCEEDS
- 24 – 26 April, Lyon, France – Participation in the INTERPOL Global Cybercrime Expert Group (IGCEG), GLACY+
- 29 April – 2 May, Vienna, Austria – Working meeting of EMPACT OAP 2019: update of the ECTEG Dark Web and Virtual Currencies Training, iPROCEEDS
- 29 April – 3 May, Dublin, Ireland – Support participation in long-distance master programme at UCD (Summer examination), iPROCEEDS

The Cybercrime Digest appears bi-weekly. News are selected by relevance to the current areas of interest to C-PROC and do not represent official positions of the Council of Europe. You receive this digest as you have taken part in Council of Europe activities on cybercrime. It is not intended for general publication.

For any additional information, contributions, subscriptions or removal from this distribution list, please contact: cybercrime@coe.int

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

www.coe.int/cybercrime