CYBERCRIME AND DIGITAL EVIDENCE IN PANAMA

*Evelyn Medina**

I. INTRODUCTION

The development of the Internet and the proliferation of computer technology has created new opportunities for those who would engage in illegal activity. The rise of technology and online communication has not only produced a dramatic increase in the incidence of criminal activity, it has also resulted in the emergence of what appear to be some new varieties of criminal activity. Both the increase in the incidence of criminal activity and the possible emergence of new varieties of criminal activity pose challenges for legal systems, as well as for law enforcement.

The cybersecurity issues have gained renewed importance since the pandemic of the new SARS-CoV-2 virus causing Covid-19 disease in Panama. Cyber-criminals have increased significantly, such as phishing, identity theft, e-mail spoofing and others, as the world becomes more interconnected, crimes of this nature are rapidly expanding.

The complex nature of cybercrime, as one that takes place in the borderless realm of cyberspace, is compounded by the increasing involvement of organized crime groups. Perpetrators of cybercrime, and their victims, are often located in different regions, and its effects ripple through societies around the world.

The restrictions imposed by governments in response to the coronavirus pandemic have encouraged victims to work from home, and even stay at home. As a consequence, technology has become even more important in both our working and personal lives. Cyberattackers see the pandemic as an opportunity to step up their criminal activities by exploiting the vulnerability of their victims working from home. Prior to the pandemic, human error was already a major cause of cyberinsecurity, employees would unknowingly or recklessly give access to the wrong people. With more people working at home, however, the problem is even greater. People were affected because names, passwords, email addresses were stolen.

Information and Communication Technologies (ICTs) permeate all aspects of life, providing newer, better and quicker ways for people to interact, network, gain access to information and learn.[1] Digitization and the emerging use of ICTs has a great impact on procedures related to the collection of evidence and its use in court. As a consequence of this development, digital evidence has been introduced as a new source of evidence. Handling digital evidence is accompanied with unique challenges and requires specific procedures. One of the most difficult aspects is to maintain the integrity of the digital evidence. Digital data are highly fragile and can easily be deleted or modified.

Digital evidence plays an important role in various phases of cybercrime investigations. In a court of law, evidence is of supreme importance; it is crucial to establish facts.

II. CURRENT SITUATION IN PANAMA

Panama is a signatory to the 2001 Budapest Convention on Cybercrime, approved by Law No. 79 of 2013. The Convention on Cybercrime, also known as the Budapest Convention on Cybercrime or the Budapest Convention, is the first international treaty seeking to address Internet and computer crime (cybercrime) by

* Prosecutor, Office of the Prosecutor of the Public Ministry, Public Ministry of Panama, Panama.

[1] https://www.thehansindia.com/business/how-digital-forensics-helping-police-gather-evidence-against-cybercrime-721668

harmonizing national laws, improving investigative techniques and increasing cooperation among nations.[2] This law refers to the convention on cyber-crime, terminologies, measures to be adopted at the national level, computer crimes, crimes related to child pornography, crimes related to infringement of intellectual property and related rights, among others.

The institution responsible for the supervision and direction of matters related to information security is the National Authority for Government Innovation (AIG) that operates under the Computer Security and Incident Response Team of Panama (CSIRC). There are two agencies responsible for the coordination and judicial investigation of cybercrime.

The Computer Security and Incident Response Team of Panama (CSIRT) is the national entity in charge of facilitating security incident response information nationwide. The CSIRT of Panama maintains close collaboration with other national CSIRT's of the region and worldwide.

Panama does not have an independent law to investigate, prosecute and punish cybercrime. The legal framework for the investigation and prosecution of cybercrime is mainly contained in the Criminal Code of the Republic of Panama in its Title VIII, on crimes against the "Legal Security of Electronic Media" categorizes crimes against computer security.

The main challenge for national criminal legal systems is the delay between the recognition of potential abuses of new technologies and necessary amendments to the national criminal law. We need to update our laws to comply with the commitments made when we signed the Budapest Convention.

At this time everyone can be a victim of cybercrime. Prosecutors need more tools and need to gain more knowledge on this topic. Every day, new technologies are created and cyberattacks are becoming more constant. We need to pursue, adjudicate, prosecute our investigations in the need to obtain quickly digital evidence, before we lose the information that most of the time are stored in other servers. In criminal investigations we need to identify the relevant evidence, followed by collection and preservation of the evidence, the analysis of computer technology and digital evidence; finally, the evidence needs to be presented in court.

The most common attempts of breach come by impersonation and are sent through emails, WhatsApp messages or by phone calls. Most criminals leave a digital footprint; a suspect's IP address, posting on a social media platform or using their mobile device for everyday use in place of a traditional computer and camera. However, this task has not been easy, derived from the difficulty of determining different aspects of the commission and persecution of cybercrime.

The Public Ministry of Panama reports a 421 per cent increase in complaints submitted relating to cybersecurity compared with 2016. Statistics indicate that the overall number increased in 2020 and 2021. From January to April 2021 Panama received 794 complaints submitted relating to cyber-crime.[3]

The following numbers have been extracted from national crime statistics and presented only to provide an insight into our country information. Furthermore, statistics only list crimes that are detected and reported. Especially with regard to cybercrime, there are concerns that the number of unreported cases is significant. The financial damage caused by cyberattacks is estimated in USD 20 thousand dollars per day.[4]

Since the pandemic, the Public Ministry have called for various awareness campaigns with national institutions to inform citizens on cyberrisks and to foster the use of best practices related to information security and the fight against cyber-crime.

Digital evidence plays a critical role in solving crimes and preparing court cases, and we often have difficulties to obtain the digital evidence in proper time. The biggest thing prosecutors were facing pre-Covid,

[2] https://en.wikipedia.org/wiki/Convention_on_Cybercrime
[3] https://ministeriopublico.gob.pa/el-ciberdelito-es-real-ministerio-publico-y-policia-nacional-lanzan-campana-de-prevencion-del-delito/#:~:text=En%20Panam%C3%A1%20de%20enero%2Dabril,solo%20en%20el%20%C3%A1rea%20Metropolitana.
[4] https://www.laestrella.com.pa/nacional/210519/cibercrimen-dispara-aumento-344-ultimos

and continue to face today, is the ability to get access to evidence. For example, in crimes against morality, Facebook did not give us a response. They argue that they only respond to serious crimes like terrorism, making it very difficult to obtain the digital evidence that we need to follow up our criminal cases.

Digital evidence is a relatively new phenomenon for law enforcement investigations and yet more cases are relying on it. Investigators are limited to their own territory, and traditional ways to obtain evidence from other jurisdictions are often not effective. This underlines the need for effective criminal justice action.

A specialized investigation unit on computer crime was created in Panama within the Directorate for Judicial Investigation, and it is under current development. This specialized investigation unit will provide capacity and training to conduct investigations and digital forensics activities.

Our country is governed by an adversarial system of criminal procedure, which raises the standard of guarantees in favour of those processed or investigated. Therefore, the more elements that are provided in the formal letter of assistance on the seriousness of the facts and the relevance of the element that is requested through international cooperation, the more likely that we can have prior or subsequent judicial authorizations, depending on what is requested.

Internet service providers (ISP) are required by Law 51 of September 2009 to provide information at the request of the prosecutors. Subsequently, it must be brought before a Judge of Guarantees, to validate the obtaining of the data.

The Office of the Prosecutor has created an action protocol, precisely, to provide all requirements with diligent, fast and efficient treatment, for which we have consulted our Office of International Affairs, our forces of order and other intervening parties, to act in a manner precise and adequate to the request made by different colleagues from other countries.

Investigating and prosecuting cybercrime requires internet-specific tools and instruments that enable competent authorities to carry out investigations. In this context, instruments to identify the offender and collect the evidence required for the criminal proceedings are essential. These instruments may be the same as those used in traditional terrorist investigations unrelated to computer technology. But in a growing number of internet-related cases, traditional investigation instruments are not sufficient to identify an offender.

Cybercrime investigations need the support and involvement of authorities in all countries involved. This is the number one barrier to prosecuting cybercrime. Most of the time, the person committing the crime is located outside of the country (or at least outside the legal jurisdiction of the court and prosecutors seeking the conviction). It is hard enough to successfully prosecute cybercriminals if they originate in the same jurisdiction as the victim, but it is close to impossible when both reside in different locations.

III. PRACTICAL CASE

A practical case that we constantly see in practice since the Covid-19 pandemic is identity theft – when criminals steal a victim's personal information to commit criminal acts. Using this stolen information, a criminal takes over the victim's identity and conducts a range of fraudulent activities in their name.

Cybercriminals commit identity theft by using sophisticated cyberattack tactics, including social engineering, phishing, malware, stealing mail, digging through dumpsters, sending SMS or WhatsApp messages to victims' cell phones. Unfortunately, most people only discover they're victims of identity theft when they attempt to open a bank account, when someone collects government benefits owed to the victim or when the cybercriminal transfers funds out of the victim's account without the victim noticing.

This chain of events often starts with one strategically written phishing email. It convinces the victims to click a link to update their password, giving the cybercriminal access to a corporate database and the victim's personal information.

IV. CONCLUSION

The investigation and prosecution of cybercrime presents a number of challenges for law-enforcement agencies. It is vital not only to educate the people involved in the fight against cybercrime but also to draft adequate and effective legislation.

The world of cybercrime is complicated. There are too many cybersecurity incidents and too few law enforcement resources available to keep up with the crime. To add more complexity to the issue, there are jurisdictional boundaries that prevent criminals from being prosecuted. Criminals may deliberately choose targets outside their own country and act from countries with inadequate cybercrime legislation.

Effectively combating, investigating and prosecuting such crimes requires international cooperation between countries, law enforcement agencies and institutions backed by laws, international relations, conventions, directives and recommendations culminating in a set of international guidelines to fight cybercrime. There are many challenges to international cooperation and establishing international guidelines to fight global cybercrime across borders.