NEW CYBERCRIMES, OLD LAWS

by

Chief Sir Gibuma Gibbs Salika ***GCL KBE CSM OBE***

Chief Justice of Papua New Guinea

Technology and its application in enhancing the quality of life for our people in Papua New Guinea (PNG) has its challenges. These realities are based on how people interact with each other through the lens of complying with the law for the preservation of good order. While the value of technology including the ushering in of what has been defined as the digital era is tremendous, it is necessary to ensure that behaviours which are counter culture to law is addressed as captured in legislation. In PNG the Cybercrimes Code Act 2016 was passed "to establish acts or omissions constituting offences committed through the use of information and communication technology or cybercrime, and for related purposes".

When we examine why laws are made, which is universally accepted for the regulation of behaviour which is deemed appropriate and anticipated to be compliant with the Constitution, we are able to understand the importance of why cybercrimes have become a topic of much discussion. I intend to approach this topic today from a practical level because I believe there are opportunities for us to explore how best our Judiciaries tackle cybercrimes while also dealing with cases of what we shall call old laws.

Concepts such as harassment which happen and impacts a person without the use of a digital instrument at times appears inconsistent with harassment which is done via a smart phone, computer or other electronic device. I am mindful that societal norms prevail in large part to what one may consider acceptable and with technological usage there have been concerns which raise the issue as to whether cybercrimes and traditional laws are so different that they may warrant different approaches to how courts tackle the problem.

All of us can accept that cybersecurity is necessary to safeguard data and protect our judiciaries from cyberattacks which compromise our ability to deliver justice. However, it is necessary to establish that old laws which have existed prior to cybersecurity legislation are still relevant and are not counter culture to the new legislation which are in place in the 21st century. The Budapest Convention "describes cybercrime as offence relating to computer-related data, fraud and network security as well as copyright infringement".

According to news reports in PNG, there are an average 10 cases of cybercrimes reported daily to the police. This indicates that there is a recognition by persons in our society that they have recourse through the judicial system in relation to threats and actual offenses emanating from cybercrimes. This augurs well for compliance in terms of persons not sitting back and accepting the past view that may have been espoused by some that when there are cybercrimes committed against them, they were limited in what they could do according to law.'

There was a 2020 case which resulted in a conviction in the National Court in which a prisoner used a fake account in prison to make threats against the Prime Minister. We have resources through the detection mechanism of the Police that provided the foundation for building the case that resulted in this successful prosecution. It is therefore relevant to note that in addressing cybercrimes in the court, without the various law enforcement agencies having the culpability to gather evidence and assist in building a good case that can be prosecuted, the court would be constrained in what it can do. Furthermore, the Public Prosecutor needs to have in place competent senior State Prosecutors to prosecute cybercrime and Fraud and corruption cases. Right now it lacks such competent and capable prosecutors.

It is argued that developments in the law usually fall behind the advances of technology. In PNG we have seen this reality and there was a time when there were scans involving people being bilked out of money in the hope of getting

more money from schemes which never materialized in what it promised. Such activities happened by the use of phones covering multiple jurisdictions prior to the introduction of legislation which made these things offences. This is an example that demonstrates the courts must be aware of the changing dynamics of the times we live and be ready to address these challenges as they present themselves in our courts. Similarly other players involved in criminal law administration must be aware of the changing dynamics of the times and be ready to address these challenges too. Here, I mention police at the forefront because they need to have competent investigators as to these very technical area of evidence gathering. Police investigators must go through very strenuous and intensive training on investigating these cyber crimes committed through technology.

The academics may wish to debate on whether there is new legal doctrine that must be reshaped with cybercrimes and old laws. I am open to getting considered views on that point but I will say that we cannot pretend in our experiences on the bench that at times some of the recent matters that are brought before us that appear seemingly novel in character can at times be perplexing to unravel given the complexity of technology and human rights and also in certain instances the lack of clarity in legislation which then become a sample of court theatrics for a distinguished Judge to preside over and make a determination.

Given my time on the bench which covers over three decades, I can say with certainty there have been radical changes in cases that come before the court that include significant technological components in criminal matters. These cybercrimes did not exist when I was first appointed to the bench and our judiciary has evolved to be able to handle any and all manner of cybercrimes that come before us. It is known that cybercrimes affect us all when we consider online transactions which are due to fraud that result in financial institutions passing the cost to all consumers in their attempt to recover such losses.

With the proliferation of Artificial Intelligence (AI) including ChatGPT which is an AI powered language model used by various sectors we can see yet again how technology is rapidly changing with legislation which has falled behind, trying to catch up and the courts then asked to help. We are now in the age of automated hacking with the use of AI which creates significant challenges for law enforcement and prosecutors added to the cross-border component given many of these types of crime may not originate in your jurisdiction but wreak havoc in your jurisdiction nevertheless. We know that cybercrime transcends borders and judiciaries should share ideas on how to address such activities.

We know that at the United Nations level there is not a consensus on cybercrime and this is itself presents challenges for our judiciaries given the international impact and cross border realities of cybercrimes and cyberattacks.

I am sure that we can all appreciate that further collaborations will allow us to engage through further discussions including questions on this topic of cybercrimes and how courts address these challenges when technology has moved far past the legislation that forms what we may call old laws. Ransomware attacks plagued some of our judiciaries in the pacific in the past four years. They continue to be a problem for some courts bringing all electronic activity to a halt due to the inability to prepare and/or combat its effect on our Information and Technology Systems.

This certainly presents an opportunity at a regional level in our jurisdictions to develop a rapid response approach that could assist in mitigating damage that our judiciaries face from cybercrimes. And while this is not the focus of this presentation, I thought it was important that I mention it for consideration.'

There are also concerns that some cybercrimes laws may adversely impact free speech. This is yet another conundrum that permeates dialog when it comes to new cybercrimes and old laws. When you have laws which may appropriately create penalties for online criminals it may face criticism where

it takes more control over the social media and potentially affects free speech. Such litigation to make constitutional determinations would likely be heard before courts to make a decision as to validity of legislation. There no doubt a wide scope of areas for which we should ponder carefully as we critically analyse how judiciaries can improve access to justice given new cyber security threats which may or may not be crimes in other jurisdiction and which may exceed the ability of existing laws.

In June 2021, the Papua New Guinea Centre for Judicial Excellence (PNGCJE) of which I am the Chairman, hosted in collaboration with the Council of Europe a training course on Cybercrime and Electronic Evidence for Judges. We have recognized the importance of facilitating training for Judges and Magistrates in this area to prepare them to handle matters as they are brought before the courts. The Cybercrime Code Act 2016 and Criminal Code Act of PNG are critical to combatting cybercrime in PNG. I anticipate that the PNGCJE will be facilitating a few more courses next year for Judges and Magistrates on the topics of Cybercrimes, Artificial Intelligence and Electronic Evidence.

Old laws are required to be repealed, amended or updated to keep up with modern times. Our ability to meet the rapid changes of these times will create certainty for court users. The pace at which technology moves in application in the world is such that the law may struggle to keep up with it. A decade ago, empirical information on cybercrime was scarce or limited in most of our jurisdictions. Laws with reference to cybercrime are still emerging.

With more data storage capacity available now, more than ever than in our history and this information potentially accessible by criminals who are hacking and using remote methodologies to illegally attempt to access, there are inherent risks associated with how we are functioning in the global community. In this vein, it is necessary to have robust laws to protect the rights of persons in ensuring that preservation of those rights is maintained and not eroded due

to harmful illegal activities emanating from the use of digital means inclusive of technology.

It is not inconceivable that a complainant may go to make a complaint at a police station in remote part of the country where they may make a report to the police only to be told they should just turn off the computer. Enforcing existing laws which do not address the reality of where we are in the digital age does not engender public confidence. The use of social media and mobile phones in PNG is regulated and as the courts hear more cases based on cybercrime legislation our jurisprudential development informs in providing metrics that can be examined with regard to the effectiveness of which the legislation has been in addressing societal behaviour that are considered norms.

Cybercrime will continue to be a challenge in our realities in PNG and I dare say throughout the world. Courts have to be able to keep up with these changes to be relevant and effective in the administration of justice and in being able to uphold the constitution. There is an expectation that with the new cybercrimes that are happening which correlates with appropriate legislation and old laws that re modernized to keep up with technology, our courts will be able to handle anything that it is required in the course of cases that are brought.

We have seen what digitalization has meant for our country over the past few decades in helping to transform our economy and provide a better quality of life for people within our jurisdiction. We also recognize that the court will continue to enhance its capacity to deal with cases as they are filed as we tackle new cybercrimes in the 21st century.