

ACUITY CYBER MOOT COURT COMPETITION, 2021

MOOT PROPOSITION

- I. Penglia is a small island country, with a population of about 50 million, surrounded by five seas. It is a small country that got its freedom from the Spartans in the year 1974, and has since been a democratic country with its own Constitution which is *in pari materia* with that of India. Penglia was facing a very serious problem of Corruption at all levels and it had no idea how to tackle this. Seeing the recent events in some other countries, the government of Penglia came up with an idea and decided that it was viable to implement it. The idea was to *first* allot each citizen with a unique number, then to make them link this unique number with their bank and then as part of the final step, to mandate online transactions so that parity is observed when entering into monetary transactions.

- II. In January 2018, the Penglia decided to allot a **Special Identification Number** (SIN) for each of its citizens in order to be better able to regulate the affairs of the country and also so that it has a track of all its citizens' monetary transactions. In pursuance of this initiative, by June 2018, Penglia had created a separate governmental institution, called the Central Authority for Special Identification Number (CASIN), for the undertaking of this task and also for storing all the data collected of all the citizens in its head office at the capital city of Penglia; Andromeda. By September 2018, the implementation plan was ready and by December 2019, the government of Penglia had established one National Center for Collecting SIN (NACSIN) each in every city in the country for the following purposes:
 - a. Collecting data and providing each citizen with a unique SIN;

ACUITY CYBER MOOT COURT COMPETITION, 2021

- b. Creating and maintaining a list of the names of the citizens with the unique SIN allotted to them; and
- c. Sending that data to the CASIN so that the information from all across the country is stored at one place.

III. On 1st January 2019, the government of Penglia released a notification mandating all the people to go to the NACSIN in their city and get a SIN within two months from the date of the notification. It took time and a lot of patience but by the end of March 2019, all the citizens of Penglia had registered with the NACSIN and had received their individual SINS.

IV. It was then that the government decided to move onto its next step; of mandating the linking of the individual SINS with the individual bank accounts of the people. The government, after due planning, on 1st May 2019 asked each citizen to link their SINS with their individual bank accounts. Since the government decided not to inform the people of their real intentions of fighting corruption, it, vide the notification dated 1st May 2020, appealed to the populous to do so in order to cater the problem of increasing number of fake bank accounts.

V. The citizens of Penglia agreed to this idea and linked their SINS with their bank accounts within two months and by 15th August 2019 the CASIN had received the data of the bank accounts of all the people. The government then decided to move on to its final step of mandating online transactions so that people had to transact from their bank accounts and since all the transactions will be recorded on the online platform available with the CASIN, there was possibility that corruption would be caught and ended in

ACUITY CYBER MOOT COURT COMPETITION, 2021

the country. Pursuant to its plan, on 15th September it released a notification saying that “from 0000 hours on 1st October 2019, only online transactions will be valid in the country and no person would be allowed to trade in cash.” The reason was given that the government wanted to make the island-nation a cashless economy. It was a welcome move by the government and by December 2019, hundreds of billions of dollars were caught that were kept in the form of black money.

VI. CASIN was responsible for collection and retention of the private information of the citizens. It was also mandated that the data cannot be shared with any third party which had the effect of breaching privacy and the sole purpose of collection of data was to mitigate the corruptive practices in the country. Since this was of national importance the CASIN had taken utmost care to protect the data of the citizens. It is complying with the security practices and procedures and has implemented ISO-270001 as its basic parameter for protecting and preserving the cybersecurity of data stored therein.

VII. Everything was going according to the plan, but on 29th February 2020, a major cybersecurity breach took place that caused the information leak from the main CASIN to some anonymous sources. The information showed that all of the bank accounts, and the details thereof, of all the citizens of Penglia were on sale on the dark web, *illegally*. This also disrupted functioning of many industries like the IT sectors, health centers who also were using the stored information for their clients and patients respectively.

VIII. Many people in Penglia received alerts that all the money in their bank accounts had been taken out and they were then left with no money with

ACUITY CYBER MOOT COURT COMPETITION, 2021

them since the country was a cashless economy and no one was allowed to keep any physical money. Some of the people also received mails stating their confirmation to withdraw cash from their accounts to which they never consented. Some also received fraud calls blackmailing them to give money or they shall leak the information to the dark web. This all caused serious mental harassment to the nations of Penglia, not just their privacy was breached but also their mental peace.

IX. There was an outrage in the populous and cries for justice were being heard all across the country. The government was tensed and an enquiry was set up to find out how the information got leaked from the CASIN's headquarters. They had the Penglia Cybersecurity Agency (PCA) that was similar to the Computer Emergency Response Team in India. PCA started the enquiry and it revealed that a cyberattack had taken place somewhere in mid-January 2020 and it had copied all the information from the database of CASIN. Following the enquiry's revelation, CASIN released a statement that it had no role in the data leak, and that a cyber-attack was the root cause of all the miseries of the people.

X. After several investigations with the cybersecurity professionals, PCA officials were able to track down three IP addresses that were being used for the purpose to launch the cyberattack and track all the personal information of the population to commit cyber-phishing and cyber-frauds.

XI. The IP addresses belonged to the Dorota Internet Service Provider (D-ISP). After further analysis this was found that the D-ISP was allocated to the Waldorf Company situated in the small state of Mango of the Penglia. While investigating it was found that the Waldorf Co. Ltd. had encrypted its

ACUITY CYBER MOOT COURT COMPETITION, 2021

data using various technologies and because of which the officials of PCA were unable to get on with their investigation.

XII. Consequently, the Director General of Penglia Cybersecurity Agency (PCA) Mr. Vander Woodsen issued a notice of 'Technical Assistance' to the Waldorf Co. Ltd. asking them to remove all the encryption technologies so that the data could be made accessible.

XIII. A Public Interest Litigation was filed against the Government of Penglia, the CASIN and all the NACSINs in the Supreme Court of Penglia, accusing them of selling the information of the people to outside sources and also for not keeping due care and caution of the data collected of the people.

XIV. The Waldorf Co. Ltd has been alleged of data breach and data theft of the citizens of Republic of Penglia. The company has also earlier tried to not allow the access of data and has also destroyed some of the data in order to protect the cyber criminals and data thieves, further to abet the crime and this has also resulted in putting the national security of the Republic of Penglia in danger.

XV. The director of the Waldorf Co. Ltd. is also charged with various cybercrimes and computer related offences. The company due to all of this has suffered huge goodwill loss and such has impacted its shares in the Penglia Stock Exchange (PSE) for which they have filed a suit against the government.

XVI. It is submitted that the Republic of Penglia has laws in place which are exactly similar to the laws of the Republic of India. It also has its Penglia Information technology Act, 2001 (PITA) in place being exactly on the same

ACUITY CYBER MOOT COURT COMPETITION, 2021

lines, mutatis mutandis, as the Indian Information Technology Act, 2000 of India. In addition, the Republic of Penglia also has a Penglia Cybersecurity and Safety Act, 2019 which is indistinguishable from the Cybersecurity Act, 2018 of the Republic of Singapore. The Republic of Penglia has its own Liability of Misuse of Computers Act, 1997 (LMCA) based exactly on Singapore's Computer Misuse Act.

XVII. The Republic of Penglia is governed by the General Data Protection Regulation (GDPR) of the European Union. The Republic of Penglia to make sure that encryption is done only to protect the secured information and not to secure unwarranted information has its own Penglia Law on Encryption, 2013 that is similar to the Australian Anti Encryption Law.

The Waldorf Co. Ltd. has been booked with;

- The various provisions of the Penglia Information Technology Act, 2001.
- Relevant provisions of the Penglia Cybersecurity and Safety Act, 2019
- Provision for abetment of crime under their Penglia Penal Code, 1920 based on lines of IPC.
- Liability of Misuse of Computers Act, 1997 (LMCA)
- Also under the relevant provisions of Constitution of Penglia and GDPR rules.

XVIII. The Waldorf Co. Ltd. has said in his defense that they are entitled to statutory immunity as an intermediary, and exempted from being exposed to potential legal consequences, including criminal prosecution. Whereas

ACUITY CYBER MOOT COURT COMPETITION, 2021

prosecution argues that they had acted arbitrarily and actively participated in conspiring, abetting and facilitating the data breach.

The matter has been listed for hearing in the Federal Court of Penglia.

Prepare arguments from both the sides.

P.S. the laws of Penglia are in pari material with those of India.

The parties are required to present their contentions on the following issues and they are allowed to add more contentions.

Issue I: Whether the Defendant has made unauthorized access and stolen the private data of the citizens?

Issue II: Whether the Waldorf Company who has been assigned the D-ISP qualified to be exempted from liability as an intermediary under §79 of the IT Act, 2000?

Issue III: Whether the Penglia Encryption Law unconstitutional?

Issue IV: Whether Waldorf Company and its officials be prosecuted for conspiring for the breach under relevant provisions of Penglia Penal Code?