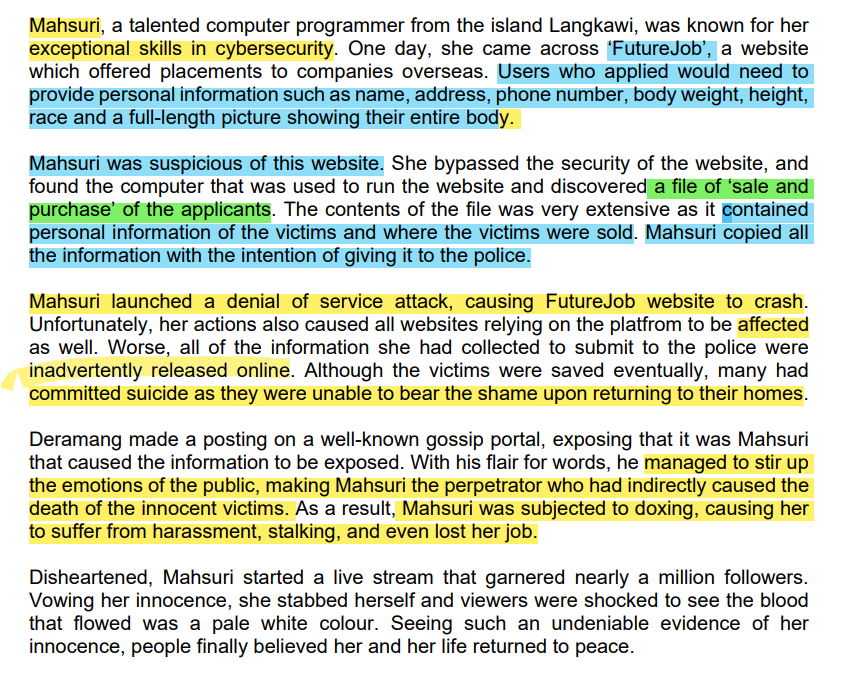
**ALTERNATIVE ASSESSMENT**

**ACADEMIC SESSION 2022/2023: SEMESTER II**

**LIA3027: Cyber Law**

**June 2023 | Time: 32 hours**

**MATRIC NUMBER: U2105281**

****

**Answer ALL of the questions below:**

1. Is Mahsuri liable under the Computer Crimes Act 1997? Why?

(5 marks)

Yes, Mahsuri would be liable under the Computer Crimes Act 1997 (CCA 1997). The Computer Crimes Act 1997 essentially by its preamble, governs and provides for offences relating to the misuse of computers. In the given scenario, we can see that Mahsuri had committed unauthorised access to a computer in which is used to run a website called ‘FutureJob’ and subsequently launched a denial-of-service attack with intention to crash the website and secure sensitive data from the aforementioned computer.

For the offences relating to Mahsuri’s potential liability under this Act, Sections 3, and 5 namely are relevant for further discussion.

1. Assuming that your answer to Question 1 is “yes”, identify and explain the offence(s) Mahsuri may be liable under the said Act.

(12 marks)

The first offence that Mahsuri may be liable under the Computer Crimes Act 1997 is the offence of committing an unauthorised access to computer material under s. **3(1) of the Act**.

To establish an accused to have committed such an offence, there are three main elements needed to be proven under paragraphs of **s. 3(1).** Firstly **para (a)** states that the person causes a computer to perform any function with the **intention** to gain access to any program or data held in any computer. Secondly, **para (b)** requires that the access itself is **unauthorized** and thirdly **para (c)** that he knows at the time when he causes the computer to perform the function that is the case.

**S. 2(2)** defines situations of a person causing a computer to perform any function to secure access to program/data where it includes subsection **(b),** he copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held**. S. 2(5)** on the other hand prescribes when an access is unauthorised when **(a)** the person himself is unentitled to control access of the kind in question to any data or program and **(b)** he does not possess consent or exceeds any right or consent to access to the program or data he has gained from the person entitled,

Applying to Mahsuri’s case, she had bypassed FutureJob’s website security, identified the computer running it and subsequently accessed the computer to find a file containing personal information of the website users being sold and purchased. After her discovery, she proceeded to copy the file contents intending to pass it on to the police. This consequently fulfils **s. 3(1)(a)** read together **with s. 2(2)(b). S. 3(1)(b)** is clear to be in affirmative in this context as she in not entitled to control access of the data nor have consent to access it by an entitled person (FutureJob) and per definition in s. 2(5), therefore unauthorised. It’s clear that she knows at the time of copying the data that she is unauthorised considering she willingly hacked into the computer and she herself is intelligent in cybersecurity field. Her claimed goodwill intention to give such information to the police is immaterial.

Thus, she may be liable if charged for unauthorised access to computer material under **s. 3(1) of the CCA 1997**.

The second offence she may be liable to under the CCA 1997 is for modification of computer contents under **s. 5(1)** through a denial of service attack.

**S. 5(1) of the Act** provides that when a person does any act which he knows will cause unauthorised modification of the contents of any computer, he/she would be guilty under this offence. **S. 2(7)** defines ‘*modification of contents of any computer’* which includes **(c)** any event occurs which impairs the normal operation of any computer. While **s. 2(8)** provides when such modification becomes unauthorised if — **(a)** the person whose act causes it is not himself entitled to determine whether the modification should be made; and **(b)** he does not have consent to the modification from any person who is so entitled.

In regard to denial of service (DoS), CyberSecurity Malaysia defines it as “a class of attacks whereby attackers attempt to bring down online services.”[[1]](#footnote-1) It includes attacks such as flooding attacks to overwhelm a system with sheer volume of traffic and crash attacks where flaws in a victim’s system is exploited and crashes. Both attacks essentially prevent entitled and legitimate users from accessing it. Legalwise, a denial-of-service attack should fall **within s. 5 of the CCA 1997** by virtue of **s. 2(7)(c)** where the modification of content includes any event occurs which impairs the normal operation of any computer, in which DoS impairs the regular operation of a server or computer running an online service/website.

Applying to Mahsuri, who has launched a denial of service attack on FutureJob. It is evident that the attack would impair the normal operation of the computer running the website, causing the website to be down and inaccessible to operators and users of FutureJob. In regard to the issue of whether that modification is unauthorised, it is also clear that Mahsuri is not entitled to make that modification or have consent to it from a person entitled e.g., from FutureJob and is aware of it. Thus, s. 5(1) should be fulfilled.

Hence, Mahsuri may be liable for modification of computer contents under s. 5(1) through a denial of service attack if she were to be charged.

(767 words)

1. Explain whether the Personal Data Protection Act 1997 is applicable to Mahsuri.

(8 marks)

The Personal Data Protection Act is a regulatory legislation that expressly seeks to regulate processing of personal data in commercial transaction and fundamentally serve to protect personal information of data subject that are in the hands of data users and processors.

**S.2(1) of the PDPA** pertains to the applicability of the Act where it states that the Act only applies to **(a)** any person who processes; and **(b)** any person who has control over or authorizes the processing of any personal data in respect of commercial transactions. Commercial transactions as defined clearly in **s. 4**, where it is transactions commercial in nature and include matters like supply or exchange of goods or services, agency, investments, financing, banking and insurance*.*

On the other hand, **S.3 provides for non-application of the Act** where it states that it does not apply to Federal and State Governments in **subsection (1)** and also non-applicable to any personal data processed outside Malaysia (unless that data is intended to be further processed in Malaysia) per **subsection (2**). Aside from the non-applicable matters expressly mentioned in **S.3**, the PDPA is also known not to be applicable to non-commercial transactions by virtue of s**. 2(1)** and credit reference agencies and personal, family and household affairs.

With reference to the applicability provisions of PDPA, we can surmise that the PDPA was intended to be applicable only to personal data processors and users in relation to commercial transactions.

In respect of Mahsuri, it does not really seem she fits in those applicable categories. She is just a computer programmer with a proficiency in cybersecurity that just happened to stumble upon a job website that has questionable practices in regard to their use and control of their user’s data and decided to take matters into her own hands. Even considering of the widespread leak of the users’ information as the unintended result of her denial of service attack, she would not be liable under the PDPA as she does not process personal data nor control and authorizes the processing of personal data in respect of commercial transactions. The purpose of the PDPA itself is to regulate the processing of personal data in commercial transactions as stated in the Act’s preamble, and to essentially protect the personal data of data subjects that is under control of data users and processors. It is more likely to hold FutureJobs liable under the PDPA as it appears to be a data user or processor.

Therefore, the Personal Data Protection Act 2010 is not applicable to Mahsuri.

(420 words)

1. What are the offence(s) that could have been committed by Deramang? Explain with reference to relevant legislations.

(15 marks)

* CMA
  + Doxing / leaking
  + S. 233(1)(a) + 505
* Penal Code
  + S. 505(b) – intent to cause alarm to public which induces against public tranquility (PT)
  + Exc – must not hv any intention versus PT
* Defamation
  + Deramang has to prove its true

1. Denial-of-Service (DoS) Attacks And Mitigation Process. (n.d.). https://siberkasa.cybersecurity.my/articles/denial-of-service-dos-attacks-and-mitigation-process [↑](#footnote-ref-1)