Information and Communication Technology Law

Lecture Title: Implications of I.T on legal processes (I)

Diploma in Law (Malta)

Lecturer: Jake Camilleri

Date: 2nd May 2022

The application of IT in the Legal Sector

1. Automated processes
2. Electronic Identification
3. Ease of research
4. Better resource management
5. Decline in risk of errors
6. Increased transparency
7. Introduction of new legal products/services

Practical Uses

1. Electronic case management
2. Online filing of documents
3. Legal Databases
4. Better client handling and delivery of services
5. Billing Software
6. Due Diligence

Ethical Concerns

- Privacy rights such as those under Regulation (EU) 2016/679:
  - Access
  - Accuracy
  - Fairness & Transparency
  - Purpose limitation
  - Integrity & Confidentiality
  - Misuse of Personal Data
- Covert tracking & Data gathering
- Spread of misinformation
- Lack of Responsibility.

Ethical Concerns

- Bias in AI Systems
- ‘Deep Fakes’
- Autonomous vehicles
- Facial Recognition
- Health tracking & automated decision making
- Neurotechnology
- Genetic engineering
- Weaponization of technology

Social Issues

- Lack of acceptance and trust in technology
- Facilitation of crime
- Gaming/Social Media addiction
- Anxiety & Depression on the rise
- Health and Fitness declining
- Lack of Socialising
- Education

Legal Considerations

- Data Privacy & Cybersecurity
  - Biometrics
  - Big Data
  - Wearable computers
  - ‘Internet of Things’
- Intellectual Property:
  - Copyright
  - Database rights
  - Trade secrets
  - Open-source software
- Net Neutrality

The application of IT in jurisprudence

- France has banned certain types of analytics of judges' decisions, to limit 'forum-shopping' by litigants.

- It now is an offence to compile and report on judges' identities in order to decipher their professional practices, aligning this practice with the processing of personal data by unlawful means.

- In serious cases, this is punishable by a maximum term of imprisonment of five years and a maximum fine of €300,000.

The application of IT in jurisprudence

- An approximate translation of the new law, Article 33, is: “The identity data of magistrates and members of the judiciary cannot be reused with the purpose or effect of evaluating, analysing, comparing or predicting their actual or presumed professional practices”.

- Under the heading “More predictable justice”, an attached report continued: “It will have to be accompanied by a regulation of the algorithms which exploit the data resulting from decisions, in order to ensure transparency of the methodologies implemented.

- “The profiling of judges and registry officials will also be prohibited so as not to undermine the proper functioning of justice”.

What Constitutes 'Cybercrime'?

- There is no official definition of 'cybercrime' however, it is widely understood as being the facilitation of traditional criminal activity (be it organised or otherwise) through the use of computer systems.

- More novel means of computer crime may only be committed through digital means (such as DDoS attacks), which only came about as computer systems became more advanced, facilitating the scale and speed at which such crimes may be carried out.

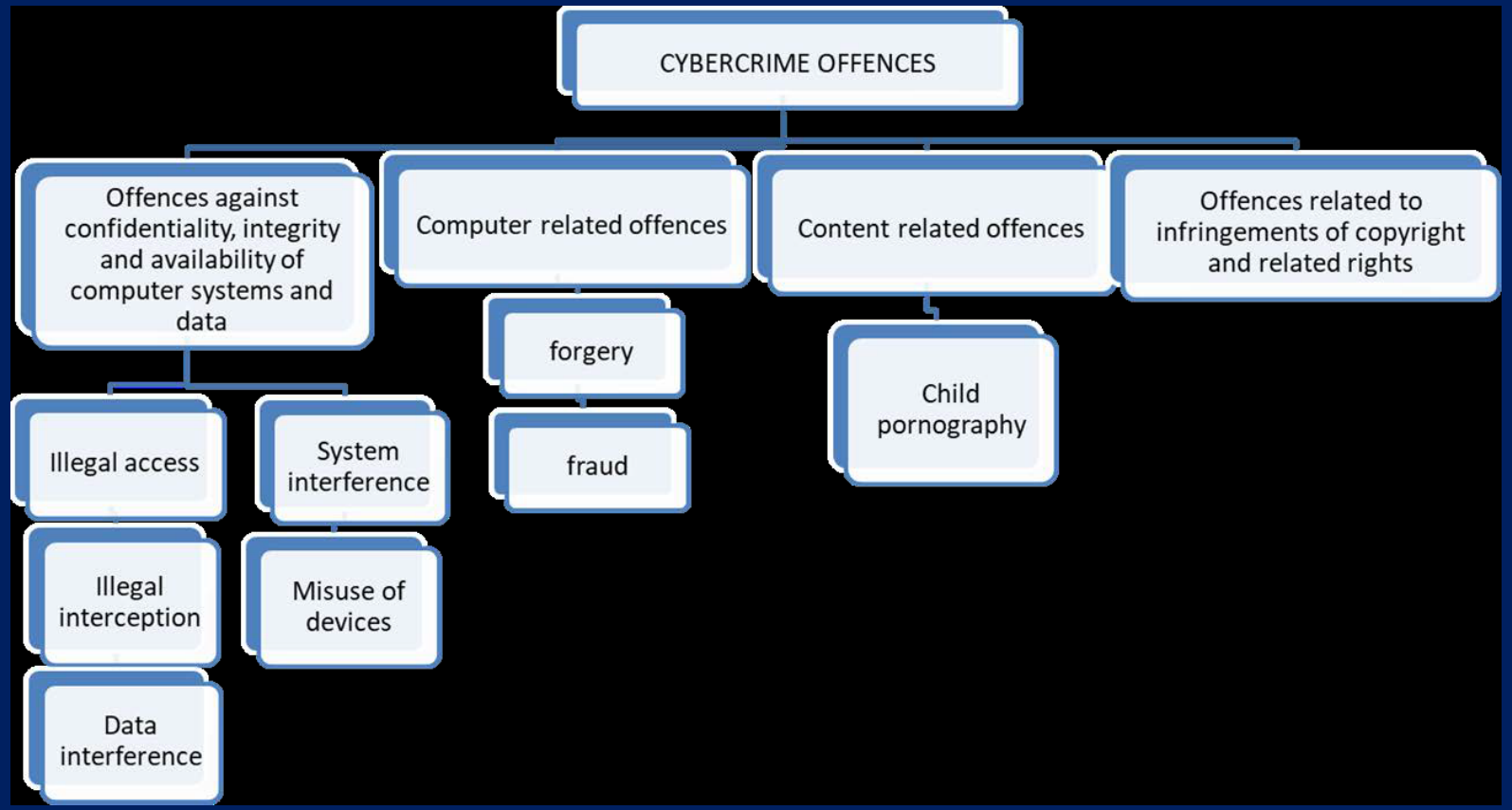
- Malta is a signatory to the Budapest Convention on Cybercrime, and has therefore implemented the provisions therein within our Criminal Code (Chapter 9, Laws of Malta).

What is Cybercrime?

- The Budapest Convention classifies cybercrime in 4 categories:

1. Offences against confidentiality, integrity and availability of computer data and systems
2. Computer-related offences
3. Content-related offences
4. Offences related to infringements of copyright

The Budapest Convention on Cybercrime



European Commission – Legal Aspects of Digital Forensics

Criminal Offences Under Maltese Law

- The old legal maxim “actus non facit reum, nisi mens sit rea” means that the criminal act along does not amount to guilt, it must also be accompanied by a ‘guilty mind’.

- The general principle within the field of Criminal Law is that **three** distinct elements must co-exist for there to be a crime:

1. The Legal Element
2. The Material Element.
3. The Mental Element.

The Legal Element

- *"Nullum crimen sine lege"* means that an action may only be deemed as a criminal offence if it is prohibited by a specific law.

- Prior to the amendments relating to computer misuse & extreme/child pornography within our Criminal Code, attributing a particular crime to an offence was tedious as our law did not cater for (now) illegal activity conducted through digital means.

- Previously, there was a valid (legal) argument to be made that an offence could not be committed as Maltese Law did not define an action (such as hacking) as a criminal offence.

The Material & Mental Elements

- The Material element is the *"actus reus"*, which means the commission of an offense by the person to be held liable.

- In certain cases, the purposeful omission could also give rise to criminal liability, provided that the other formalities are present.

- The Mental element is the *"mens rea"* or the 'guilty mind' with which the act is done. This is a procedural necessity and cases are dismissed typically on this basis, as it is particularly difficult to prove a persons' malintent.

Various Forms of Cybercrime

- Computer Fraud
- Phishing
- Hacking
- DDoS
- Malware
- Trojans and other viruses
- Ransomware
- Sexploitation
- Cyberterrorism
- Child Pornography
- Infringement of Intellectual Property rights.

Computer Misuse

- Malta's Criminal Code (Chapter 9, Laws of Malta) regulates computer misuse through 337B-337H
- Based on the UK Computer Misuse Act and the Budapest Cybercrime Convention
- Drafted and defined broadly to account for 'all' scenarios

Computer Misuse

- Definitions
- Unlawful access to, or use of, information
- Misuse of hardware
- Commission of an offence outside Malta
- Offences and Penalties
- Search and Seizure

Interpretation – Art. 337B(1)

- "**computer**" means an **electronic device** that performs logical, arithmetic and memory functions by manipulating electronic or magnetic impulses, and includes all input, output, processing, storage, **software** and communication facilities that are connected or related to a computer in a **computer system** or **computer network**;

- "**computer network**" means the interconnection of communication lines and circuits with a computer through a **remote device** or a **complex** consisting of two or more **interconnected** computers;

- "**computer output** " or "**output**" means a statement or a **representation of data** whether in written, printed, pictorial, screen display, photographic or other film, graphical, acoustic or other form produced by a computer;

Interpretation – Art. 337B(1)

- **computer software**" or "**software**" means a computer **program, procedure or associated documentation** used in the **operation** of a computer system

- "**computer supplies**" means punched cards, paper tape, magnetic tape, disk packs, diskettes, CD-roms, computer output, including paper and microform and any storage media, electronic or otherwise

- "**computer system**" means a **set of related computer equipment, hardware or software**

Interpretation – Art. 337B(1)

- "**function**" includes logic, control, arithmetic, deletion, storage, retrieval and communication of data or telecommunication to, from or within a computer;

- "**supporting documentation**" means any documentation used in the computer system in the construction, clarification, implementation, use or modification of the software or data.

Unlawful access to, or use of, information – Art. 337C

A person who without authorisation does any of the following acts shall be guilty of an offence

a) **uses** a computer or any other device or equipment to access any data, software or supporting documentation held in that computer or on any other computer, or uses, copies or modifies any such data, software or supporting documentation;

b) **outputs** any data, software or supporting documentation from the computer in which it is held, whether by having it displayed or in any other manner whatsoever;

c) **copies** any data, software or supporting documentation 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;

d) **prevents** or **hinders access** to any data, software or supporting documentation;

e) **impairs** the operation of any system, software or the integrity or reliability of any data.

Unlawful access to, or use of, information – Art. 337C

f) **takes possession** of or makes use of any data, software or supporting documentation;

g) **installs**, **moves**, **alters**, **erases**, **destroys**, varies or adds to any data, software or supporting documentation;

h) **discloses** a password or any other means of access, access code or other access information to any unauthorised person;

i) **uses another person's** access code, password, user name, electronic mail address or other means of access or identification information in a computer;

j) **discloses** any data, software or supporting documentation unless this is required in the course of his duties or by any other law.

Misuse of Hardware – Art. 337D

Any person who, **without authorisation**, does any of the following acts shall be guilty of an offence:

a) **modifies** computer equipment or supplies that are used or intended to be used in a computer, computer system or computer network.

b) **takes possession** of, damages or destroys a computer, computer system, computer network, or computer supplies used or intended to be used in a computer, computer system or computer network or impairs the operation of any of the aforesaid.

Commission of an offence outside Malta – Art. 337E

- If any act is committed outside Malta which, had it been committed in Malta, would have constituted an offence against the provisions of this Sub-title, it shall, if the commission affects any computer, software, data or supporting documentation which is situated in Malta or is in any way linked or connected to a computer in Malta, be deemed to have been committed in Malta.

Offences and Penalties – Art. 337F

1. Fine shall not exceed €23,293.73, or to imprisonment not exceeding **four** years, or to **both** such fine and imprisonment.

2. When such offense is directed towards the Government or a public authority the penalty shall range from €232.94 and €116,468.67 or to imprisonment from **three** months to **ten** years, or to both such fine and imprisonment.

Subsequent offences shall be fined at a minimum of € 1,164.69

Offences and Penalties – Art. 337F

3. Penalties shall also apply when committed by an employee to the prejudice of their employer.

4. If a person produces any material or acts in preparation or furtherance of an offence, the same punishment shall be awarded.

5. Accomplices or any person who aids or abets the commission of an offence shall be equally liable.

6. The burden of proof lies on the party alleging authorisation and this burden shall not be considered to have been discharged with the mere uncorroborated testimony of the person charged (hence further proof is required).

Search, Seizure & Retention – Arts. 337G & 355P

- **337G**: The Minister may, for the purposes of this Sub-title, by regulations prescribe:

a) the manner in which the Police may search computers, computer systems or computer supplies and seize data or software stored therein;

b) procedures and methods for handling evidence that is in an electronic form.

- **355P**: The Police, when **lawfully** on any premises, may seize anything which is on the premises if they have **reasonable grounds** for believing that it has been obtained in consequence of the commission of an offence or that it is evidence in relation to an offence...and that it is necessary to seize it to prevent it being concealed, lost, damaged, altered or destroyed.

Computer Data & Retention – Arts. 355Q & 355S

- 355Q: The Police may, in addition to the power of seizing a computer machine, require any information which is contained in a computer to be delivered in a form in which it can be taken away and in which it is visible and legible.

- 355S: Anything which has been lawfully seized by the Police may be retained so long as is necessary in all the circumstances.

- (2) Without prejudice to the generality of the aforesaid, anything lawfully seized by the Police under this Code may be retained for use as evidence at the trial or for forensic examination or any other aspect of the investigation, or in order to establish the thing's lawful owner.

- (3) The Commissioner shall provide for the proper custody of anything seized.

Extreme Pornographic Content

- Amendments to the Criminal Code following UK's promulgation of new laws regulating extreme pornographic content.

- Article 208D prohibits the distribution, display in a public manufacturing, printing, or otherwise makes or introduces into Malta any 'extreme' pornographic images shall be liable to imprisonment for a term between **18** months to **3** years or to a fine between **€3,000** and **€6,000**, or to both imprisonment and a fine.

- This also applies to any person who "keeps" or "acquires" such images. Therefore, the downloading and storage of such images is an offence under Maltese Law.

What is Considered 'Extreme'?

- S.L 9.05 states that n image will be deemed as 'extreme' if it portrays, in an explicit and realistic way:

  - an act which takes or threatens a person's life.
  - an act which results, or is likely to result, in a person's severe injury.
  - rape or other non-consensual penetrative sexual activity.
  - sexual activity involving, directly or indirectly, a human corpse.
  - an act which involves sexual activity between a person and an animal or the carcass of an animal.

Pornographic Content Depicting Minors

- Article 204(c) and (d) of the Criminal Code imposes a term of imprisonment between **five** and **ten** years upon whosever:

  (c) knowingly causes, for sexual purposes, a person underage to participate in real **or simulated** sexually explicit conduct or exhibition of sexual organs, **including through information and communication technologies**, or

  (d) knowingly **attends a pornographic performance** involving the participation of a person under age.

- The inclusion of 'simulated' sexually explicit content includes scenarios such as 'Deepfakes' or 'pseudo-images' which depict minors.

- For the purposes of the Code, visiting websites containing pornographic material constitutes viewing of a 'pornographic performance'.

What about Viewing?

- Downloading and storing explicit material on one's device is a clear case of possession. However, there is a divide between scholars on whether 'viewing' constitutes simple 'possession' for the purposes of the Criminal Code.

- Every time a new web page is viewed, many of its images and videos are downloaded to a folder on the hard drive. These temporary internet files, or **cache files**, are used by the computer to load web pages more quickly in the future.

- Depending on the amount of internet use and the space allocated for these files, these images and videos can remain on a hard drive for months or years.

What about Viewing?

- Courts will seemingly adopt the 'intent-based approach'. This means that factors such as search history, numerous website visits and the duration thereof play a key role in determining the accused's intent to view the indecent material.

- The UK previously utilised a 'classification system' ranging from 1 to 5, to determine the severity of the explicit image ([2003] EWCA Crim 2766 'Regina V. Oliver & ORS').

- In the case of [2004] EWCA Crim 449 'Regina V. Beaney', multiple files depicting sexual activities with minors were retrieved from one of the computer's directories, having been automatically stored by the browser.

What about Viewing?

- The previously mentioned system has been replaced by a categorisation system, as pictured below (UK Sexual Offences Guidelines). This has been implemented to streamline the complexities of overlapping levels.

	Possession	Distribution*	Production**
Category A (previously levels 4 and 5)	Possession of images involving penetrative sexual activity	Sharing images involving penetrative sexual activity	Creating images involving penetrative sexual activity
	Possession of images involving sexual activity with an animal or sadism	Sharing images involving sexual activity with an animal or sadism	Creating images involving sexual activity with an animal or sadism
Category B (previously levels 2 and 3)	Possession of images involving non-penetrative sexual activity	Sharing of images involving non-penetrative sexual activity	Creating images involving non-penetrative sexual activity
Category C (previously level 1)	Possession of images of erotic posing	Sharing of images of erotic posing	Creating images of erotic posing

* Distribution includes possession with a view to distributing or sharing images
** Production includes the taking or making of any image at source, i.e. the original image
Making an image by simple downloading should be treated as possession for the purposes of sentencing

What about Accidental Viewing/Downloading?

- Using certain software computer forensics experts may retrace the steps that led to a file being downloaded. Often, a link can be found between innocent search terms and the name of the illegal file. If the file was acquired through a P2P network, an expert can survey the shared folder and find that the contents are otherwise legal.

- Certain file properties will indicate when the file was created (or downloaded), when it was last changed, and when it was last accessed. If an expert finds that the file was created and last accessed at the same time, it is quite possible the user was unaware of the file because it was never accessed after the initial download. If the file was last accessed within an hour of the creation timestamp, this suggests the user deleted it shortly after download.

- The retrieval of internet browsing history can also establish a user's online habits **(digital fingerprint)** and create a timeline of events leading up to an accidental download.

Grooming

- Article 208AA of the Criminal Code imposes imprisonment not exceeding **six** years on any person over eighteen years who "meets of communicates on one or more occasions" with a person under the age of **sixteen** years, intending to do anything to or in respect of the said person.

- The above includes scenarios where the offender proposes to meet or arranges to meet the victim.

- The formal requirement is that the alleged offender should not "reasonably believe" that the person they are meeting is over the age sixteen.

Questions

1. What is the most common expression used in the literature to describe crimes committed using technology? (**Computer crime**/ **Cybercrime**/ **Online crime**/ **Digital crime**)
2. Is there a precise definition for the above that is agreed upon in the international law? Mention 5 different forms of such.
3. Which of the following is a requirement for establishing a criminal offence under the principle of legality? **(Customs**/ **Written Rules**/ **Habit**/ **None)**?
4. What are the elements which need to be proven for an act to be considered as a criminal offence?
5. What are the legal terms for the abovementioned elements?
6. How are these elements linked? Are there any procedural 'pit-falls'?
7. What considerations do Courts make in determining the severity of a crime?

The Maltese Cybercrime Unit

- The Cyber Crime Unit is a specialised section within the Malta Police Force set-up in 2003. It primarily provides technical assistance in the detection and investigations of crime wherein the computer is the target or the means used.

- Not limited to criminal acts associated with technology, but extends to investigations of more traditional offences such as fraud, threats and other serious crimes but also assists in the analysis of digital evidence seized in connection with investigations as well as in identifying persons who are committing crimes over the internet.

- Works closely with a number of international organisations and law enforcement agencies.

EUROPOL and EC3

- The European Cybercrime Centre (EC3) was set up by Europol to strengthen the law enforcement response to cybercrime in the EU.

- At the level of operations, EC3 focuses on the following types of cybercrimes: **cyber-dependent crime, child sexual exploitation** and **payment fraud.**

- The support provided extends also to tackling criminality on the Dark Web and alternative platforms.

J-CAT

- The Joint Cybercrime Action Taskforce (J-CAT), was launched in September 2014. Located at Europol's European Cybercrime Centre (EC3), it helps fighting cybercrime within and outside the EU.

- Intelligence-led, coordinated action against key cybercrime threats and targets by facilitating the joint **identification**, **prioritisation**, **preparation**, **initiation** and **execution** of **cross-border investigations** and operations by its partners.

- J-CAT Members include EU and Non-EU States, and their tasks includes:
  - selecting the most relevant proposals;
  - sharing, collecting and enriching data on the cases in question;
  - developing an action plan, which is led by the country that submitted the selected proposal;
  - going through all the necessary steps to ensure the case is ready to become a target of law enforcement action — a process that involves consulting with judicial authorities, the identification the required resources, and the allocation of responsibilities.

Combatting Cybercrime

- Legislation enacted as a deterrent to commit the offence with proportionate punishments depending on the severity of the crime. The issues with this are that laws merely act as a deterrent and that defending parties may use certain procedural technicalities to delay the judgment or have it dismissed.

- There is also the standard of 'innocent until proven guilty' within Criminal Law, which must be proven by the alleging party. This causes timely delays to any sentence being adjudicated upon, particularly with the compilation of 'best evidence'.

- Legislation imposing industry standard certification (particularly for cybersecurity) is one way of combatting the 'hands-on' attacks such as hacking, which relates to the physical and virtual infrastructure implemented by organisations.

- Educating both youths and adults to safeguard their digital identity and minimise their digital fingerprint could combat against cybercrime such as ransomware, malware, fraud and identity theft as attackers typically target older individuals who would not be as tech-savvy.

Combatting Cybercrime

- Increased collaboration and information sharing between supervisory authorities may dampen the affect and longevity of any crimes as assailants will be found more effectively.

- Jurisdictional issues may be remedied through multi-lateral agreements between contracting states, setting a definite jurisdictional framework and defining which Court will have jurisdiction, to speed up the litigation process.

Legal Challenges

- Identifying which activities can be considered illegal ("*Nullum crimen sine lege*").
- Enacting criminal law relating to computers and the Internet.
- Identifying the offenders and victims of the crimes.
- Enforcement, particularly with **preservation of evidence**, **jurisdiction** and the **international aspect** of the crimes.
- "adequate punishment" and how to quantify damages in the digital age.

Case Study

- You are part of Malta's cybercrime unit (the "Unit") and have been tracking the activities of a rogue group of hackers "F-Society", lead by a certain "Mr. Robot". The Unit has been informed that F-Society have performed their largest hack to-date, infiltrated the largest conglomerate "E-Corp" and accessing the personal data of millions of innocent people.

- The personal data included victims full names, health data, financial data, usernames and passwords to various E-Corp services.

- When going through E-Corp's servers, you notice that there is a vast amount of pornographic content, some even including minors, however, you suspect that this was planted by F-Society to incriminate E-Corp.

- The Unit has caught Mr. Robot, who has since been held for questioning, and have also initiated proceedings against F-Society.

Case Study

1. How should the Unit handle these series of events?
2. Do you foresee any legal or procedural issues?
3. Should this incident be handled alone?
4. On what basis should the Unit charge the assailants?
5. What repercussions could Mr. Robot and F. Society face, if charged?
6. Are there any repercussions on E-Corp for having the explicit images on their servers?

Any Questions?

- Remember, there are no stupid questions, only stupid answers.

Diploma in Law (Malta)

21 LAW

CAMILLERI PREZIOSI
ADVOCATES

MAMO TCV
ADVOCATES