Computing related legislation

Countries have different laws, and sometimes it is hard to prove in which country an offence was committed, and equally as hard to trace the offender and prosecute them.

Many new applications are invented and some of them can be used to commit the offence, many of these offences have no legislation.

Legislators must balance the rights of the individual with the need for security and protection from terrorist or criminal activity.

E.g. many countries have legislation banning the use of strong cryptography.

Computing related legislation:

Legislation to privacy is broadly categorised into laws intended to protect privacy and those which have been passed in the interest of national security, crime-detection and counter-terrorism.

Laws that relate specifically to computing:

The data protection act (1998): which is designed to ensure that personal data is kept accurate, up-to-date, safe and secure and not used in ways that could harm individuals.

The Computer Misuse Act: which makes it an offence to access or modify computer material without permission.

The regulation of Investigatory Powers Act (2000): which relates to the powers of public bodies to carry out surveillance and investigation, and intercept communication.

Other laws:

Copyright, Designs and Patents Act (1998) – more general application in protecting the intellectual property rights of works such as books, music, art, computer programs etc.

Combating computer-related crime

Cybercrime is a complex and difficult task with technology evolving at an exponential rate and policing them requires officers to have a high level of technical proficiency.

One of the biggest issues is the time it takes to draft and enact legislation prohibiting the use of certain technology when the speed of developing technology is so fast.

(a) The Data Protection Act 1998

Anyone who stored personal details must keep them secure from malicious or unauthorised access.

The eight principals (LEARN):

1. **Data must be processed fairly and lawfully**
2. **Data must be adequate, relevant and not excessive**
3. **Data must be accurate and up to date**
4. **Data must not be retained for longer than necessary**
5. **Data must be kept secure**
6. **Data can only be used for the purpose that it is collected for**
7. **Data must be handled in accordance to people's rights**
8. **Data must not be transferred outside the EU without adequate protection**

All data users must register with the Data Commissioner

Three key people involved in the Data Protection act

1. **The Information Commissioner** is the person whom parliament has empowered to enforce the act.
2. **The data controller** is a person or company that collects and keeps the data about data subjects.
3. **The data subject** is the person who has data stored about them.

(b) The Computer Misuse Act (1990)

This is primarily designed to prevent unauthorised access or 'hacking' of programs data.

a) **Unauthorised access to computer material.**

b) **Unauthorised access with intent to facilitate a crime.**

c) **Unauthorised modification of computer material/intent to impair operation of a computer.**

d) **Making, supplying or obtaining anything which can be used in computer misuse offences.**

c) The Copyright , Designs and patent act (1998)

This act protects creators of books, music, art, programs and video from having their software illegally copied.

The act made it illegal to use, copy or distribute commercially available software without buying the appropriate licence.
When a computer system is designed and implemented, licencing must be considered in terms of which software you use.

e.g.
If you use a commercial piece of software for music production, it may not be permissible to then go on to sell your finished product without paying the company a small fee for every copy of a song you sell.

Similarly, if a subscription to office is brought, it is not permitted to install it on multiple computers without buying a multi-user licence.

If you buy a song/music CD or software/video/game. It is illegal to:

- Distribute free copies of that work
- Make a copy and sell it
- Use the software on a network unless the licence allows it

Software companies can take some measures to prevent illegal duplication:

- The user must enter a unique licence key to install the software
- Some software will only run provided the CD is present in the drive
- Some applications only run when a special piece of hardware called a dongle, is plugged into the USB port.
- Some pieces of software have a limited subscription so the software will not function after a given time period unless it is renewed.

d) The Regulation of Investigatory Powers Act (2000)

This act regulates the powers of public bodies to carry out surveillance and investigation and covers the interception of communications. It was introduced to take account of the growth of technology, the Internet and strong encryption.

Additions have been made in 2003 & 2010, with the latest draft bill put before Parliament in 2015 November.
It particularly focuses on electronic surveillance, the legal decryption of encrypted data and the interception of electronic communications by security services, the Secret Intelligence Service and the Government Communications Headquarters (GCHQ). Under the act, they can intercept emails, access private communications and plant surveillance devices.

The Act:

i. Enables the government to demand that an ISPs provide access to a customer's communications in secret.

ii. Enable mass surveillance of communications in transit.

iii. Enables certain public bodies to demand ISP's fit equipment to facilitate surveillance.

iv. Enables certain public bodies to demand that someone hand over keys to protected information.

v. Allows certain public bodies to monitor people's internet activities in compliance with Human Rights act 1998.

vi. Prevents the existence of interception warrants and any data collected with them from being revealed in court.