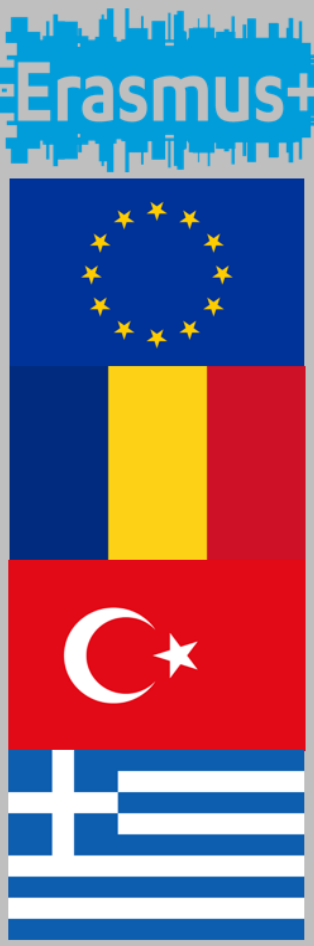
PROTECT YOUR DIGITAL WAY TODAY AND TOMORROW



Chania, Crete, Greece
9 – 13 March 2020

LOOK OVER
CYBER-SECURITY'S
KEYWORDS
&
LOCK!

Cyber-Law in Greece

CYBERCRIME LEGISLATION

Before defining the concept of cybercrime, we must first define the area in which it is committed.

The internet, ICT and networks are referred to ,as cyberspace.

Cyberspace is defined as the fictional environment in which computer network communication occurs.

People can also be considered interconnected by computers, regardless of physical geography.

The word <cyber> comes from the Greek word <commander>.

Cyberspace is not just the internet, software and informative systems, but also the people and social interaction within these networks

The Internet is all the interconnected computers around the world, which are in a common communication network and exchange messages (packets) using different protocols (standard rules of communication).

It appears in the early 1990s and begins to spread and develop rapidly.

This connection enables users to access the data, information and content of all these networks.

To access the internet ,you need a computer and a modem connected to a phone line.

Historically speaking, the internet was designed in 1963 by Roberts, who created it as a form of intercom without the slightest external interference.

The great boom of the internet began with the introduction of the World Wide Web at the CERN research institute in 1989.

Social media first appeared on the internet in 1994.

The goal of the first hybrid Social Networking sites was to support their users' communication through chat rooms and personal websites ,where they could publish and share personal thoughts, ideas and information.

In 2004 Facebook was created. Its development was very fast.

2006 was the year that Facebook stopped addressing solely to the American college community.

As a result, it was directed at all internet users freely, while allowing individual social networks to be formed and thus connecting users and social networks .

The internet , more particularly, social media have enhanced and facilitated human interaction and consequently communication.

The global nature of the internet leads to an immediate exchange of people's views across the globe.

Unfortunately, the anonymity it offers hides a variety of risks.

On the one hand, the more space it occupies in our daily lives, the more opportunities it offers to both the citizens and the corporate world.

On the other hand, it multiplies the risks of developing criminal activities.

It is estimated that 1.5 billion users, about 24% of the global population, are connected to the internet, for all kinds of activities, such as product purchase, online services (e-commerce, e-banking, etc.), research for information , news (search engines like Google, Yahoo, blogs, newspaper portals, e.t.c.

USERS ‘ PROFILE

The average user has a particularly high level of education: Not only 62% has a university degree, but also a postgraduate degree.

Looking at internet access rates based on the sample demographic characteristics, it appears that men, young people, especially those aged 16-24, high educated people and residents of large urban centers excel in using the internet.

ELECTRONIC CRIME

According to the Cybercrime Prosecution, "cybercrime" is considered a criminal offense that is committed by using computers and data processing systems and it is punishable by specific penalties under the Greek law.

The Interpol calls cybercrime digital and divides it into three categories:

Firstly, into cybercrime, which includes piracy, data theft and time theft, the so-called computer break-ins.

Secondly, into the one related to banking fraud and thirdly, into cybercrime which includes child pornography, drug dealing and money laundering.

- It is also important to make a distinction between those, who commit such crimes. A resentful ex who makes abusive status on facebook is ,by no means, the same as a cracker or an online scam.
- In the first case, we talk about people who do not necessarily have special computer skills, whereas the jurisdictional issues (e .g communication of the Greek authorities with facebook) are to some extent regulated.
- Yet, more often than not, the cybercriminals who cause the most serious problems in states, organizations and individuals, are highly intelligent individuals with the knowledge and equipment that make it extremely difficult to be identified.

CATEGORIES OF ELECTRONIC CRIME

The basic distinction made between cybercrimes, is the one between computer crime and cybercrime.

It must be taken into consideration, that according to the Greek legal system, there is no law that deals exclusively with internet issues and regulates the behavior of internet users in terms of criminal law.

As computer crimes, the Greek criminal law defines the illegal copying of confidential data (FP 370B), the illegal use or access to computer programs or data, including hacking (FP 370B).)and computer fraud (PC 386A).

In case these crimes are committed in an internet environment (Cybercrime), these articles also apply to specific cases.

A distinction - that may help to better comprehend cybercrime -can be made on the basis of whether they are targeted directly at a computer, e.g. computer virus, or if they are facilitated by the use of computer networks and devices, having a different purpose, e.g. fraud, identity theft.

FREQUENT FORMS

Cybercrime can take many forms, while in Greece the main ones are:

a. Internet fraud (e.g credit cards)
b. child pornography
c. cracking and hacking
d. software-piracy
e. trafficking
f. trafficking in narcotics and weapons
g. crimes in chat rooms, facebook, etc. (e.g.child molestation)
h. cyberbullying
i. incitement to homicide or suicide
j . the illegal acquisition of personal data
k. spam
l. e-phishing

Mobile phones can be considered as other forms of cybercrime.

Data can be retrieved even with the use of a mobile phone via Bluetooth. The fact that the handset can be remotely controlled, makes it easy to make calls that can cost a great deal , not to mention that one can elicitate calls.

Video games could also be included in the forms of cybercrime.

Wireless access and data processing capabilities combined with the use of specialized software help in hacking and remote computer management.

Finally, ATMs are also a means of committing cybercrime, since there have been many ways to steal passwords from time to time, either by installing a micro-camera or by blocking card mechanisms.

It has also been observed the process of placing identical keyboards on the actual keypad to extract the codes.

Some cybercrimes can be committed online, since having such an extensive network is very helpful.

For example, juvenile pornography, which exists and is being prosecuted even off-line, has risen due to the proliferation of the Internet.

Respectively, many cybercrime offenses are prosecuted under existing criminal code provisions, such as bullying, blackmail and defamation (simple and slanderous).

CHARACTERISTICS OF ELECTRONIC CRIME

Cybercrime has features that need to be taken into account in order to be better understood.

It is fast, it is committed in seconds and it is often not even realized by the victim.

It's easy to do, of course for those who know it, while the traces it leaves behind are digital ...

To do so , it requires excellent and specialized knowledge.

It can be performed without moving the offender , the person who acts from the comfort of his office or home through his computer away.

It enables people with specialties, such as child pornography, to communicate quickly or in real time, without having to move away, easily, inexpensively, being crowded in the same news groups or in chat rooms ..

"Cybercrime" criminals do not often appear with their real identities, they send e-mails with false information.

It is a cross-border crime and its effects can occur simultaneously in many places.

It is very difficult to determine its location and it is also quite difficult to investigate and locate the perpetrator. The perpetrator may be located in country A and the evidence may be in a different and distant country or may be located in several different countries at the same time.

- The investigation normally requires the cooperation of at least two states (the state in which the result of the criminal conduct was perceived, and the state where the evidence is located). Cases of criminal behavior within a single state are rare.
- The record of cybercrime does not correspond to reality as few cybercrime cases are reported internationally. As a result, the magnitude of cybercrime is "even darker" than in "common" cybercrime.

DeepWeb (also known as Deepnet, Undernet, the invisible Web or the Hidden Web) refers to the content of the World Wide Web that does not belong to the Surface Web, which is found by a regular search engine.

The darknet (or dark network) is an overlay network, accessed only by specific software, configurations, or licenses, often using non-standard communications protocols and ports.

Encryption is the process of encrypting a message or information in such a way that only authorized parties can access it and those who are not authorized cannot.

Cloud storage is a web data storage model where data is stored on remote sites.

ELECTRONIC CRIMES

Financial fraud online

Online financial fraud mainly takes place in the form of online shopping.

There is no law in our national law that defines crimes exclusively on the Internet. However, Law 1805/88 has added provisions to the Penal Code for crimes committed by computers, such as computer fraud (386A Penal Code).

So, when these crimes are committed on the Internet, these laws are again applied.

Verbal Abuse and Defamation

Defamation and slander are standardized as criminal offenses.

The term is used to describe particularly abusive, even threatening behavior, as well as comments that are usually offensive and have direct or indirect consequences on a person's psychological state (e.g. isolation, anxiety, fear or insecurity).

Online child abuse and exploitation

Online child sex trafficking continues to be the most alarming aspect of cybercrime with volumes of material ,which would be totally incomprehensible ten years ago, partly because of the growing number of young children accessing Internet-enabled devices and social media.

Offenders are constantly looking for new ways to avoid law enforcement, including anonymization and encryption tools.

Most of the material is on the internet, but some of the most extreme material is in secret services that can be accessed through darknet.

The live stream of child abuse remains a highly complex crime that needs to be investigated into and is likely to increase further in the future. It often leaves behind little trace of forensics.

The turnover of child pornography industry on the internet is more than three billion euros a year.

The number of websites that host pornographic minors, even infants, is estimated to have increased by 345% over the last decade.

The daily traffic of some of such web content is around 150,000.

In Greece, websites with similar content have been growing since 2001 and then 150% per year.

The importance of reporting illegal content is vital in order to help child victims not live the same trauma over and over, but to make the internet safe for all of us and our children.

The public in Greece can report either by using their name or anonymously on the HotLine.gr website or on DIECP.

Violent and racist content

- Racism and xenophobia are often encountered in the internet world through the publication of opinions or data aimed at reducing or inciting discrimination or violence against people identified on the basis of characteristics such as race, color, and religion.
- Law 4285/2014 introduces Article 81A into the Penal Code which standardizes racist crime. This article specifically provides for higher penalties for crimes committed "out of hatred on the grounds of race, color, religion, ancestry, national or ethnic origin, sexual orientation, gender identity or disability." .

Privacy of Communications

The inviolability of the privacy of communications is protected by Article 19 of the Constitution. However, our communication with internet users is compromised when someone violates our passwords on our social media or e-mail.

In the Greek legal system many laws have been adopted concerning the privacy of communications, such as Law 3471/2006 on the protection of personal data and privacy in the field of electronic communications, law 3431/2016 which concerns inter alia Electronic Communications and law 2225/1994 on the protection of freedom of association.

The declassification the confidentiality of communications is only permitted for the detection of particularly serious crimes.

Internet terrorism

Terrorism has been a growing phenomenon in recent years. The internet is now an important weapon in the hands of the next generation of terrorists.

Terrorism is defined as cyberonline (cyberterrorism) <a deliberate, politically motivated attack on information, computer systems, computer programs, and data that results in sub-ethnic groups committing violence against civilian targets.

The new General Regulation (EU) 2016/679 of the European Parliament and of the E. Council of 27 April 2016 <on the protection of individuals with regard to the processing of personal data and on the free circulation of such data>, was adopted in Greece.

The use of electronic evidence in court has long been concerned with Greek case law and theory, which have to deal with the lack of specific procedural rules and the fact of conflict of interest.

Clearly, evidence that infringes the right to privacy or the right to freedom of expression and communication contradicts, at first sight, the provisions of the Constitution.

PRIVACY

Personal data of any living natural person, that is, any information concerning an existing natural person or any information that may directly or indirectly identify a natural person, in particular by reference to an identity such as name, ID number, address, or details concerning the physical, psychological, economic or social condition of such natural person.

The court accepts as evidence, text messages (considered letters) in e-mail, messenger or facebook, as well as photos, movie shows, phonographs and all kinds of mechanical imagery.

Any interference with these documents is considered to be falsification.

DIECP

The Directorate of Electronic Crime Prosecution (DIECP) reads purely cases of genuine cybercrime (e.g. 'Computer fraud', Article 292A P.C. or "obstruction of the operation of information systems", as applicable, etc.) and if their investigation requires specialized technical or digital research.

Website cyberkid.gr

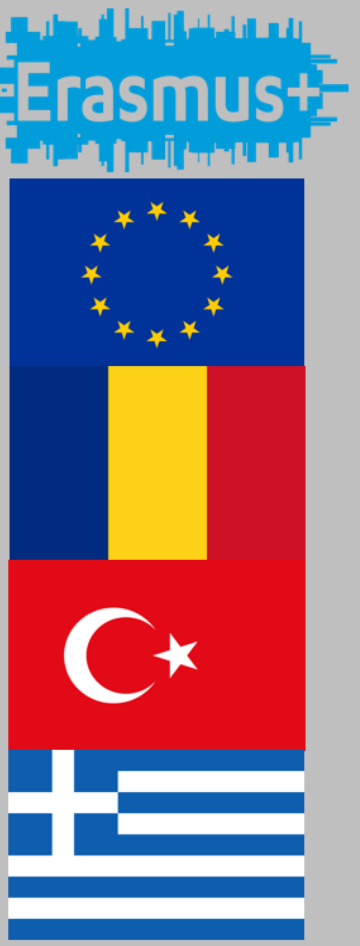
Www.cyberkid.gr provides useful information and tips on how the whole family can take advantage of the benefits of modern technologies and of course the internet.

In addition, the site was enriched with two new sections. **The 'Cyber Alert' section** where the public can be informed of the most frequently occurring dangers that circulate online, and the **"News" section** where announcements regarding the Directorate of Electronic Crime Prosecution are posted.

The internet has been accused of playing a role in deaths.

- Brandon Vedas died of an overdose of a mixture of legal and illegal drugs spurred on by his IRC counterparts.
- Shawn Woolley killed himself with a pistol for reasons related to his addiction to EverQuest.
- Armin Meiwes was stabbed to death and ate part of Bernd Jürgen Brandes' body when the latter responded to his first request for a "big man ready to be slaughtered and eaten."

PROTECT YOUR DIGITAL WAY TODAY AND TOMORROW



Chania, Crete, Greece
9 – 13 March 2020

LOOK OVER
CYBER-SECURITY'S
KEYWORDS
&
LOCK!

Cyber-Law in Greece

Thank You!