uc3m | Universidad Carlos III de Madrid

Cybercrime

Academic Year: (2023 / 2024) | **Review date: 24-04-2023**

Department assigned to the subject: Criminal Law, Procedural Law and History Law Department

Coordinating teacher: OTERO GONZALEZ, MARIA PILAR

Type: Electives ECTS Credits : 3.0

Year : 1 Semester : 2

REQUIREMENTS (SUBJECTS THAT ARE ASSUMED TO BE KNOWN)

Bachelor degree in Law.

Knowledges of Criminal Law are required.

OBJECTIVES

That the students can apply the broader (or multidisciplinary) acquired knowledge and ability to solve problems in new or unfamiliar environments within contexts related to their field of study

Which students are able to integrate knowledge and handle complexity, and formulate judgments based on information that was incomplete or limited, includes reflections on social and ethical responsibilities linked to the application of their knowledge and judgments

Which students can communicate their conclusions and the knowledge and rationale underpinning to specialists and non-specialists in a clear and unambiguous

That students possess learning skills that enable them to continue studying in a way that will be largely self-directed or autonomous.

-Write Quality legal reports

-Demonstrate Who have assimilated the basic methods and principles of research activity in the criminal procedure legal field

-Manage Sources of legal information specific to the Criminal Justice

-Develop Scientific and legal texts and carry out the analysis of them effectively

-Apply Knowledge of criminal and procedural institutions in performing legal functions

To understand the stages that lead to criminal court conviction and possibilities of influence on it under the presumption of innocence;

Informing the adequacy of research methods in a criminal offense and the adequacy of the sources of evidence and adequacy of the evidence in relation to the concrete theory of the case.

-Discriminar The elements of each of the main theoretical model of criminal prosecution and its influence on contemporary criminal legal systems;

Demonstrate the assumption of different procedural roles, prosecution, defense and prosecution arguments and strategies according to the same

To understand the stages that lead to the solution of a problem of general and special criminal law related to this matter and master the theoretical instruments at its disposal to achieve more accurate decision or most favorable to the interests they defend

-Apply Skills professions linked to the exercise of criminal legal practice

TEACHING METHODS

Detection of criminal risks in the field of new technologies of information and communication technologies (ICTs). adequate legal reaction and legal measures against criminal risks identified in the activity of new technologies.

They know the state of the case law of European criminal courts to provide legal solutions to specific issues that may arise in practice.

You can expose the complex picture of the transnational nature of this crime, what their characteristics and their role in the field of crime as a whole.

You can set what offenses main way associated with cybercrime, as well as the most suitable mechanisms to fight, by criminal law against those organizations are.

You can properly integrate national regulation on Cybercrime in the panorama of Comparative Law and especially in international standards.

Cybercrime: The appearance of this subject is warranted against rising crime committed through the Internet, affecting legal interests ranging from heritage and socio-economic order, sexual inviolability of minors and incompetents, privacy, intellectual property and industrial, etc. On this subject the phenomena that affect crime in the network, the impact of the complexity of the new forms of technology and data protection, and the need to generate effective responses, such as the confiscation will study, criminal responsibility of persons legal, and regulation of banking secrecy to discourage the commission of these crimes.

CYBERCRIME. CHALLENGES OF CRIMINAL LAW TO THE TICS

I. INTRODUCTION. POLITICAL CONSIDERATIONS CRIMINALS. DATA cybervictimization.
1. The Criminal Law in tow of new technologies: risk society. Increase in crimes of abstract danger. Deformalization. Expansion. Pedagogical profile.
2. Influence of Internet on criminal law.
3. Dark Side of development: new forms of criminality, use of computer networks to facilitate the commission of conventional crimes, macrovictimización, problems incrimination competition problems anonymity sense of impunity. Platform organized crime.

II. INTERNATIONAL LEGAL FRAMEWORK.

III. LEGAL ASSETS AFFECTED BY THE CYBER CRIME.
Privacy, honor, freedom, sexual freedom and indemnity, property, intellectual property, external and internal security of the state. Special reference to the criminal protection of privacy and heritage in relation to crime in cyberspace.

IV. COMMUNICATION TECHNOLOGIES. DATA PROTECTION AND RISKS TO THE COMMUNICATION TECHNOLOGIES.
1. Evolution of privacy: Theory of the spheres. Privacy and impact of new technologies: active right to self-determination linked to control. Telephony networks expansion. postindustrial society: Modern professional secrecy. The right to anonymity. The right to oblivion.
2. Crisis of the public. Invocation of self-regulations.
3. Criminalization of auditory and visual clandestine control illicit communication control signals: signal interception, conversations, violation password.
4. Special cases: Video cameras in public spaces. Eavesdropping. Hidden cameras and recordings in which the party is involved. inconsentida dissemination of intimate videos. Requirements judicially authorized tracks: jurisprudential analysis.
5. Data Protection: habeas data computer.

V. BLOCK AS PLATFORM FOR CYBER CRIME ORGANIZED CRIME.
1. Organized crime and criminal sociology: concept and characteristics. Typologies. Organizational structure. Corruption, globalization, sophistication. State-organized crime connection.
2. Rationale for specific criminal response to organized crime. Basis. Legally protected. Incentives collaboration with justice.
3. Legislative technique criminal. criminal types. insolvency problems.
4. Response alleging that the crime would not result provechoso¿: confiscation, money laundering, international agencies autonomous control of finances. Tax havens and secrecy jurisdictions.

VI. INFORMATION TECHNOLOGY. Illegal activities.
1. Crimes whose only means of commission is the Network: hacking, computer sabotage (cracking). Special reference to denial of service (Denial of Service).
2. Traditional Infractions using such networks as a tool: internet fraud (phishing), spoofing treatment, espionage (Spyware), attacks on intellectual property (Linking, Inlining, metatags, keywords), attacks on property very personal we made through Internet with or without ICT: cyberbullying, child grooming, sexting.
3. Attacks by the broadcast content: child pornography, cyberterrorism.

VII. ALLOCATION OF CRIMINAL LIABILITY TO INDIVIDUALS AND LEGAL FOR PUBLICATION OF CONTENTS CRIMINAL (CONTENT PROVIDERS, SERVICE PROVIDERS).

VIII. Prosecutability. Competition concerns.

During the two weeks of online learning, the students shall review and study the materials, power points , judgments and the audiovisual material provided. They must also solve a practical case.

Tutorials : The tutorials will be conducted daily through Skype or email.

- Attendance Part In Madrid: the students shall attend the activities, conferences and seminars planned.

ASSESSMENT SYSTEM
ORDINARY SESSION:

- Up to 15% participation in the forum

- Up to 45% resolution of a case study or report

- Up to 40% multiple-choice exam

The student must obtain at least a mark of 3 out of 6 in the continuous assessment (forum and resolution of a practical case / report), and 1.8 out of 4 in the multiple-choice exam. If he/she does not obtain this score, he/she will be failed and will have to attend the extraordinary exam.

EXTRAORDINARY EXAM:

- 100% Examination.

% end-of-term-examination:	40
% of continuous assessment (assigments, laboratory, practicals…):	60

BASIC BIBLIOGRAPHY

- Brett Shavers cybercrime case presentation using digital forensics and investigative techniques to identify cybercrime suspects, Oxford: Syngress, 2013
- Otero, P. ¿   ¿Criminal law and the risks posed by Internet. An examination of Spanish Criminal law en Juan Cayón Peña -edit.- Security and defence: ethical and legal challenges in the face of current conflicts, Springer, 2022
- Otero, P. Cyberspace: a platform for organized crime in Cyberspace Risks and Benefits for Society, Security and Development Editors: Ramírez, J. Martín, García-Segura, Luis A. (Eds.), Springer, 2017