

<b>Course Title</b>	Criminal Law and New Technologies				
<b>Course Code</b>	DLNLT505				
<b>Course Type</b>	Compulsory				
<b>Level</b>	Master (LLM)				
<b>Year / Semester</b>	2 <sup>nd</sup> / Fall				
<b>Teacher's Name</b>	Dr Aikaterini Sykioti, Prof. Ioannis Inglezakis				
<b>ECTS</b>	10	<b>Lectures/week</b>		<b>Laboratories/week</b>	
<b>Course Purpose</b>	<p>The aim of this course is to highlight the influence of new technologies in the field of criminal law, the risks to the rights and freedoms of the individual, as well as the benefits for the administration of criminal justice. In addition, it aims to delve into the various crimes committed in cyberspace, as well as the complex issues that arise in the field of criminal procedure, mainly through the use and utilization of new technology systems, but also the use of digital evidence.</p>				
<b>Learning Outcomes</b>	<p>Upon successful completion of the course, students will be able to:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> <b>Describe</b> the legal dimensions of cybersecurity breaches and their impact on the administration of criminal justice.</li> <li><input type="checkbox"/> <b>Interpret and apply</b> substantive and procedural criminal law principles to crimes committed through new technologies and the internet.</li> <li><input type="checkbox"/> <b>Critically analyze</b> the characteristics, severity, and penalties of various categories of cybercrimes.</li> <li><input type="checkbox"/> <b>Handle</b> cybercrime cases both in and out of court, demonstrating the effective management of digital evidence and procedural safeguards.</li> <li><input type="checkbox"/> <b>Evaluate</b> the roles and mechanisms of national, European, and international cooperation bodies in combating cybercrime.</li> <li><input type="checkbox"/> <b>Demonstrate</b> specialized knowledge of privacy and data protection in the context of cybersecurity and criminal investigations.</li> <li><input type="checkbox"/> <b>Develop</b> strategic approaches and legal problem-solving techniques for addressing emerging challenges in cybercrime regulation.</li> <li><input type="checkbox"/> <b>Assess</b> new procedures and legal frameworks for protecting fundamental rights and legal goods in the digital environment.</li> </ul>				

	•		
<b>Prerequisites</b>	-	<b>Corequisites</b>	-
<b>Course Content</b>	<p>This course includes the following modules:</p> <p>1. Introductory data on the influence of Artificial Intelligence in the administration of Criminal Justice.</p> <p>The first module aims to get to know the students of the course, to explain the diagram, the content, the requirements of the course and the obligations of the students, and the explanation of the assignments/activities and methods of evaluation of the course. Also, the framework for communication, cooperation and interaction between me and students is defined. Time is given to resolve students' questions. At the same time, the concepts of artificial intelligence and cyberspace, as well as their relationship with criminal law and the administration of justice, are introduced. In particular, the benefits and risks for rights and freedoms in the context of criminal law and the administration of criminal justice are examined.</p> <p>2. Cybercrimes against property - computer fraud, obstruction of information systems, money laundering.</p> <p>In the second section, reference is made to legal and ethical issues arising from the use of new technologies, at national and European level. The various cybercrimes are categorized, with an analysis of the offences of the criminal code relating to offences against property, with emphasis on computer fraud and the obstruction of the operation of information systems. A further analysis of the area of financial crime, and in particular money laundering, follows.</p> <p>3. Crimes against sexual freedom and minors committed online. Cyber harassment.</p> <p>In the third section, the issues related to crimes against sexual freedom and minors via the Internet are presented, i.e. the crimes of the Criminal Code committed in the field of information technology. An analysis and interpretation of the relevant provisions of the Criminal Code concerning these offences, with the recent changes that have taken place in them under European legislation, is presented. At the same time, the causes of these and the basic concepts of "harassment cyber surveillance" and "cyber harassment" are analyzed.</p> <p>4. Criminal Procedural Law and new technologies - digital evidence and digital evidence.</p> <p>In the 4th section, aspects of Criminal Procedural Law as well as European Criminal Law and International Cooperation in Cyberspace are analyzed, highlighting the key points of the criminal procedure and the role of the involved bodies in the justice process, both at national and European/international level.</p>		

	<p>In addition, the issues raised by the specificities of crimes committed with computers are investigated at a procedural level, and specifically through an in-depth analysis of terms such as "digital evidence", "digital traces" and "digital evidence". Furthermore, the role of the above in the administration of criminal justice is examined, and related aspects such as the seizure of digital data, the procedural guarantees of investigative acts and investigations in cyberspace, as well as the part of invalidities. Furthermore, the way in which digital evidence is used and presented in criminal proceedings is investigated, as well as their evaluation by the judge.</p>
<b>Teaching Methodology</b>	Remotely
<b>Bibliography</b>	<p><u>(a) Bibliography</u></p> <p>M. Gbandi, Kaiafa, "Artificial Intelligence as a Challenge for Criminal Law – In Search of a New Model of Criminal Liability?" in Criminal Chronicles, 2023, Issue 1, p. 3 - 13.</p> <p>Th. Dalakouras, "Definitions and substantive provisions for the criminal treatment of cybercrime" in "Cybercrime", 2023, Law Library, p. 25-42.</p> <p>M. Gbandi, Kaiafa, "Criminal Law and Abuses of Informatics", Armenopoulos, 2007p. 1058-1087.</p> <p>I. Igglezakis, "Informatics Law", 5th ed. 2024, Sakkoulas Publications.</p> <p>M.Kaiafa-Gbandi, "The criminal treatment of attacks against information systems" in "Elements of EU Criminal Law", Second Edition, 2019, p. 150-170.</p> <p>Charalampakis A., "Concise Interpretation of the Criminal Code, After the Changes of Law 5090/2024", Law Library, 2024, p. 328-329 and 449-450.</p> <p>Morosinis I.K. in Dalakouras Th. "Cybercrime", "The transfer of money using electronic banking services as criminally punishable behavior in the light of crimes against property and property in its timeless dimension The "removal" and "appropriation" of accounting money as computer fraud", Nomiki Bibliothiki, 2023, p. 131 -182.</p> <p>A. Sykiotis to A. Charalampakis "The New Penal Code, Interpretation according to Article of Law 4619/2019", 2nd Volume 2025, Law Library, p. 3010-3021 (a. 337), 3033-3047 (a. 339 of the Criminal Code), 3077-3083 (a. 346 of the Criminal Code), 3088-3096 (a. 348A of the Criminal Code)</p> <p>N. Koumoulentzos, "Child Pornography", Law Library, 2023, p. 101 – 174.</p> <p>Charalampakis A., "Concise Interpretation of the Criminal Code, After the Changes of Law 5090/2024", Law Library, 2024, p. 378.</p> <p>Th. Dalakouras, "Cybercrime", 2023, Law Library, p. 399-595.</p>

	<p>Th. Dalakouras, "The new Code of Criminal Procedure, Summary Interpretation of Law 4620/2019" - Volume Two (Articles 462-592), Law Library, 2020, p. 209-210.</p> <p>Papadopoulos, L. Th., 2020, "Cybercrimes", Law Library, p. 23 -180.</p> <p><u>(b) Resources</u></p> <ul style="list-style-type: none"> <li>• <a href="https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:52018DC0237&amp;from=EN">https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:52018DC0237&amp;from=EN</a></li> <li>• Papapanagiotou, A. &amp; Zachou, C., (2021). Justice systems. The ethical dilemmas and the limits of the European Charter of Ethics. <a href="https://www.esdi.gr/wp-content/uploads/images/stories/pdf/epimorfosi/2021/zachou-papapanagiotou_2021.pdf">https://www.esdi.gr/wp-content/uploads/images/stories/pdf/epimorfosi/2021/zachou-papapanagiotou_2021.pdf</a></li> <li>• Tassis, S., (2019), Law in the Age of Artificial Intelligence, <a href="https://www.lawspot.gr/nomika-blogs/spiros_tassis/dikaio-stin-epohi-tis-tehnitis-noimosynis">https://www.lawspot.gr/nomika-blogs/spiros_tassis/dikaio-stin-epohi-tis-tehnitis-noimosynis</a></li> <li>• Artificial Intelligence: Opportunities and Threats (2020), <a href="https://www.europarl.europa.eu/news/el/headlines/society/20200918STO87404/techniti-noimosuni-eukairies-kai-apeiles">https://www.europarl.europa.eu/news/el/headlines/society/20200918STO87404/techniti-noimosuni-eukairies-kai-apeiles</a></li> <li>• Kanellou, L., (2020), Artificial Intelligence at the Service of a Smart Justice, <a href="https://www.lawspot.gr/nomika-nea/i-tehniti-noimosyni-stin-ypiresia-mias-exypnis-dikaiosynis">https://www.lawspot.gr/nomika-nea/i-tehniti-noimosyni-stin-ypiresia-mias-exypnis-dikaiosynis</a></li> <li>• Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combating violence against women and domestic violence <a href="https://eur-lex.europa.eu/legal-content/el/ALL/?uri=CELEX:32024L1385">https://eur-lex.europa.eu/legal-content/el/ALL/?uri=CELEX:32024L1385</a></li> </ul> <p>Daliani, F., (2023), Artificial Justice: The Presence of Artificial Intelligence in the Administration <a href="https://www.lawspot.gr/nomika-nea/techniti-dikaiosyni-i-paroysia-tis-tehnitis-noimosynis-ston-horo-tis-aponomis-dikaiosynis">of Justice, https://www.lawspot.gr/nomika-nea/techniti-dikaiosyni-i-paroysia-tis-tehnitis-noimosynis-ston-horo-tis-aponomis-dikaiosynis</a></p> <ul style="list-style-type: none"> <li>• Kofinis, S., (2021), From Digital Justice to Digital Judge: Can Artificial Intelligence Replace Judges?, <a href="https://www.esdi.gr/wp-content/uploads/images/stories/pdf/epimorfosi/2021/kofinis_2021.pdf">https://www.esdi.gr/wp-content/uploads/images/stories/pdf/epimorfosi/2021/kofinis_2021.pdf</a></li> </ul>
<b>Assessment</b>	<p>Final written exam, 2 assessment assignments, 2 assessment online interactive discussions, a variety of weekly educational activities such as interactive activities and self-assessment activities.</p>

	<p>Final examination (50%)</p> <p>2 assessment assignments (15% + 20% = 35%)</p> <p>2 online interactive activities (7.5% + 7.5% = 15%)</p>
<b>Language</b>	Greek/English