Co-funded by the Erasmus+ Programme of the European Union

DIGICRIMJUS

New challenges
for teaching, researching and practicing criminal law in the digital age
2020-1-HU01-KA203-078670

Digicrimjus: Master of Laws (LL.M.) in Digitalization and Criminal Law

Course Plan

1. General Introduction as IO2

The trilateral program set out here represents against the long and intense partnership of the institutions prior to the applied program the very unique possibility to start its own and very unique "master program on criminal law and digitalization" (CIS standing for Constance, Istanbul, Szeged as well as for Criminal, Intelligence, Science). The curriculum set out here is the foundation for that LL.M. program. It is planned that future students may obtain an own specific master degree on comparative and digital criminal law when successfully obtaining a BA or equivalent degree from one of the three law schools, or a comparable degree from another University after an entrance qualification (1), then taking part within one of the trilateral seminars organized by the leading partners and successfully passing it (2), participating and passing courses on digital criminal law hosted at the University of Szeged and delivered by academic staff of the partner institutions (IO01) (3), and eventually writing one master thesis (4).

This program is as a trilateral program unique in its kind. That underlines the transnationality of "digital questioning". Also, the program is setting a specific emphasis on the further development of comparative law and especially on different methods of comparative work and seeks to make aware of the many different ways of comparative research. It addresses the top tier law students and students of computational science of the three institutions and beyond to further develop their skills and to educate the future experts in digital criminal law. Including the program into the just founded institute of computational intelligence and law in Konstanz, in the future, it will be possible to also include further studies of data protection, international contracting, as well as questions of legal theory and philosophy into the Master program.

The Digicrimjus: Master of Laws (LL.M.) in Digitalization and Criminal Law is a is a one-year program designed to provide students with the skills and knowledge necessary to navigate the increasingly complex intersection of digital technology and criminal law. The curriculum combines coursework in law, technology, and data analytics to prepare graduates for careers in law enforcement, cybersecurity, and related fields.

2. Curriculum and Course Plan

Term I.					
Subject	Course type (Lecture / Tutorial)	Contact hours (hpw)	Assessment	Credits	Lecturer
Core Concepts of Criminal Law in the European Digital Area	L	13	Exam	4	Prof. Dr. Krisztina Karsai / Prof. Dr. Adem Sözüer / Prof. Dr. Liane Wörner
Introduction to Legal Informatics (Data Analytics for Criminal Law)	T	16	Term mark	5	Adrienn Princz, Nicolai Preetz
Digitalization and Criminal Law I. (General Part)	L	16	Exam	5	Dr. Andor Gál
Cybersecurity Law and Policy	L	13	Exam	4	András Lichtenstein
Digital Ethics and Social Responsibility	L	13	Exam	4	Dr. Batuhan Baytaz / Pinar Özcan
Introduction to Digital Data Protection	L	13	Exam	4	Dr. Szilvia Váradi
Seminar in Digitalization and Criminal Law	T	13	Term mark	4	Prof. Dr. Krisztina Karsai / Prof. Dr. Adem Sözüer / Prof. Dr. Liane Wörner

Term II.					
Subject	Course type (Lecture / Tutorial)	Contact hours (hpw)	Assessment	Credits	Lecturer
Advanced Legal Informatics (AI and Criminal Law)	T	13	Term mark	4	Adrienn Princz, Nicolai Preetz

Digitalization and Criminal Law II. (Special Part)	L	13	Exam	4	Prof. Dr. Krisztina Karsai
Digital Currency and Financial Crimes	L	11	Exam	3	Yigit Yeniyetisme (Sascha Daul)
Digitalization and Criminal Procedure	L	13	Exam	4	András Lichtenstein
Cybercrime Investigation and Prosecution	T	11	Term mark	3	Prof. Dr. Adem Sözüer
Digital Evidence and Forensics	T	11	Term mark	3	Csaba Anti
Privacy and Surveillance Law	L	11	Exam	3	Prof. Dr. Liane Wörner
How to write a thesis	T	12	Pass/Fail	0	Prof. Dr. Krisztina Karsai / Prof. Dr. Adem Sözüer / Prof. Dr. Liane Wörner
Masters Thesis	n.a.	n.a.	Exam	6	Academic Supervisor

3. Short description of courses

Term I. Courses:

Core Concepts of Criminal Law in the European Digital Area: The course provides an introduction on how lawmakers and law enforcement agencies work to keep pace with the rapid changes in technology and the online environment. Core concepts include: Cybercrime, Data Protection, Intellectual Proprety, Online Speech, Jurisdiction and Procedural rights in the EU.

Introduction to Legal Informatics (Data Analytics for Criminal Law): Legal informatics plays a crucial role in the development and enforcement of criminal law. This course is aimed at the use of data analytics techniques and tools to analyze legal information and support decision-making processes in the criminal justice system. Topics covered include legal databases and other tools used to manage and analyze legal information, as well as data mining.

Digitalization and Criminal Law I. (General Part): The course focuses on the impact of digitalization on criminal law, specifically the general part of criminal law. The general part of criminal law deals with the basic principles of criminal law, such as criminal liability, culpability, and punishment. Topics include the concept of criminal liability in the digital age and the legal definition of cybercrime and its various forms.

Cybersecurity Law and Policy: The course covers the crucial topics in ensuring the security and integrity of digital systems and protecting the privacy and personal information of individuals and organizations both from a legal as well as a policy and governance perspective.

Digital Ethics and Social Responsibility: The course provides an introduction to the moral and ethical considerations involved in the use of technology and digital resources. These are crucial in ensuring that technology is used in a way that benefits individuals and society as a whole, while also protecting the privacy and rights of individuals and promoting ethical behaviour in the digital world. The legal and ethical issues raised by the use of artificial intelligence in criminal justice are also covered.

Introduction to Digital Data Protection: A solid understanding of digital data protection principles and practices is essential for anyone who handles or manages sensitive information in today's digital world, especially in the criminal justice system. This course covers the protection digital data from unauthorized access, use, and disclosure. It also involves understanding the legal, technical, and organizational measures required to safeguard sensitive information and maintain its confidentiality, integrity, and availability.

Seminar in Digitalization and Criminal Law: The trilateral seminar organized by one of the project partners is aimed at deepening student's already acquired knowledge in the field of Digitalization and Criminal Law. It also serves as a practical project-based task, where students gain in depth experience in comparative digital criminal law and law in action.

Term II. Courses:

Advanced Legal Informatics (AI and Criminal Law): This is a is a specialized course that explores the intersection of artificial intelligence and criminal law. It covers the technical (e.g.: machine learning, natural language processing, and predictive analytics), ethical, legal, and social implications of using AI in criminal law, including issues related to privacy, bias, transparency, and accountability. Students will learn about the various AI tools and techniques used in criminal law, such as predictive policing, facial recognition, and automated decision-making systems.

Digitalization and Criminal Law II. (Special Part): With a focus on the special part of criminal law, the course covers the impact of digitalization on criminal law, including the emergence of new forms of criminal activity, such as cybercrime, online harassment, and identity theft. Students will learn about the legal framework for regulating digital crimes, including international and national laws and regulations.

Digital Currency and Financial Crimes: This specialized course that focuses on the use of cryptocurrencies, such as Bitcoin, and their role in financial crimes. It covers the basics of digital

currencies, including their history, technology, and use cases; as well as the various ways in which digital currencies can be used in financial crimes, including ransomware attacks, investment scams, and darknet marketplaces. Students will also learn about laws, regulations and best practices, such as the Anti-Money Laundering (AML) and Know Your Customer (KYC), that are designed to prevent financial crimes such as money laundering and terrorist financing.

Digitalization and Criminal Procedure: This introductory course is designed to cover the various ways in which digital technologies have changed the criminal justice system, including the investigation, prosecution, and trial of criminal cases. It also covers the challenges of conducting criminal trials in a digital age, including the impact of digital media on witness credibility and testimony.

Cybercrime Investigation and Prosecution: This specialized practical course (tutorial) framework surrounding cybercrime investigations and prosecutions, including international and national laws and regulations. Students will learn about the challenges of investigating and prosecuting cybercrimes, including case-studies related to jurisdiction and evidence gathering.

Digital Evidence and Forensics: This practical course (tutorial) covers the issues related to evidence gathering and the use of emerging technologies in criminal investigations. Students will learn about the various tools and techniques used in digital forensics, such as data recovery, analysis, and preservation, and the considerations that need to be taken into account when using these techniques.

Privacy and Surveillance Law: This specialized course covers the issues surrounding privacy and surveillance in modern society, including constitutional law, data protection laws, surveillance laws and criminal procedure implications. Students will learn about the use of various surveillance technologies, such as CCTV cameras, drones, and facial recognition systems, and the implications for individual privacy and civil liberties. The relevant criminal procedure framework is also covered.

How to write a thesis: This preparatory seminar gives an overview of the various steps involved in writing a thesis from selecting a research topic and conducting a literature review, to analysing data and presenting findings. It is aimed to provide students with the skills and knowledge they need to successfully complete their and to deepen their critical thinking and analytical skills that are valuable in any academic or professional setting.

Master's Thesis: The Master's Thesis is the zero-credit compulsory capstone project in completing the Digicrimjus: Master of Laws Programme (LL.M.) in Digitalization and Criminal Law. It is a comprehensive research paper that demonstrates the candidate's ability to conduct original research and contribute to the academic and professional discourse in Digitalization and Criminal Law.