PROPOSAL FOR THE INTRODUCTION OF THE NEW COURSE IN THE CURRICULA OF THE FACULTY OF LAW OF THE UNIVERSITY OF ZAGREB

1. COURSE TITLE

Cybersecurity and cybercrime

2. HOURS OF LECTURES

30 hours

3. NUMBER OF ECTS

4 ECTS

4. LECTURERS

Prof. dr. sc. Dražen Dragičević; dr. sc. Marko Jurić; dr. sc. Hrvoje Lisičar; dr. sc. Tihomir Katulić; dr. sc. Nina Gumzej

5. COURSE DESCRIPTION

a) Summary

In contemporary world, it is almost impossible to differentiate between physical and digital. Digital culture of today is integrated in physical reality and in all material objects of man’s everyday activity and life - production, trade and financial business, education, science, culture, entertainment and all other social activities. All these invisible goods and connections constitute an area, so called Cyberspace, which has become increasingly important from the legal and public policy perspectives. In these contexts, issues of cybersecurity and cybercrime cannot be avoided. Cybersecurity is an issue which transcends legal regulation. Its achievement depends on the proper implementation and use of a series of technical, procedural, organizational and legal measures. On the other side, fighting cybercrime is becoming an increasingly important task of legal science and legislation, in terms of prevention, detection and repression. However, there is also a need to reconcile the effectiveness of cybercrime prosecution with the need to ensure fulfillment of fundamental human rights. In this context, there is a danger that excessive criminalization might, apart from preventing the undesirable phenomena, suppress and undermine human rights and the rule of law. Therefore, in addition to proper strategy on cybersecurity, it is extremely important to develop real sense of potential threats in the field of cybercrime, and legal measures aimed at suppressing them.
b) Detailed description of the course


4. Introduction to cybercrime and law. The concept of cybercrime. Historical development of cybercrime. From computer crime to cybercrime. Global, regional and national regulations in the field of cybercrime. Activities of international organizations in the field of cybercrime and cybersecurity - United Nations, Council of Europe, Organization for Economic Co-operation and Development, International Telecommunication Union. (3 hours)


7. Cybercrime and protection of human rights and liberties. Balancing the enforcement of cybercrime legislation with the protection of human rights and liberties. Conditions and safeguards under the Convention on Cybercrime (article 15). Data preservation v data retention. (3 hours)

8. Cooperation in the field of cybersecurity and prevention of cybercrime. Cybercrime as a global issue. International cooperation under Cybercrime convention. Public-private cooperation in the field of cybersecurity. (3 hours)

9. Recapitulation and assessment. (3 hours)

6. GENERAL AND SPECIFIC KNOWLEDGE

By the end of the course, students should be able to:
- understand the concepts of cybersecurity and cybercrime on both theoretical and practical levels;
- understand concepts of technical, organizational, procedural and legal measures in the context of
cybersecurity, and their interaction;
- have deep understanding of the specific challenges cybercrime poses for the contemporary societies and the role and limits of law in its repression;
- have deep and working knowledge of the legal framework field of cybercrime and specifically of the Convention on cybercrime as a core international legal tool for fight against cybercrime

7. FORMS OF TEACHING

In-class lectures combined with an e-learning module.

8. ASSESSMENT

Assessment consists of two parts:

1) (A) Written essay on the topic determined jointly by the student and the teacher or (B) Written exam (70% of the grade), and
2) Oral exam (30% of the grade)

9. LITERATURE

Students will be provided with all the necessary materials on the first class and via e-learning module. Compulsory literature shall include:

1. Dragičević, Kaspersen, Schwerha, Article 15: Conditions and Safeguards under the Budapest Convention on Cybercrime, COE 2012. (selected chapters), available online
2. Dragičević, Jurić, Article 15 – Safeguards in the Eastern Partnership region, COE 2013. (selected chapters), available online
3. Comprehensive Study on Cybercrime, UNODC 2013. (selected chapters), available online

10. QUALITY CONTROL

Regular self-assessment of teaching staff and assessment by the students at the end of semester, in the form of anonymous questionnaire. Results of the assessment shall be made public via department’s website.