# Privacy and security

## Prof. Vittorio Bachelet; Prof. Ennio Alagia

***COURSE AIMS AND INTENDED LEARNING OUTCOMES***

The aim of the course is to make students aware of the current importance of personal data protection, privacy and security, introducing the key principles and legal institutes in this area. The goal to acquire up-to-date tools to understand this developing sector cannot disregard, firstly, the consideration of the recent changes introduced at the European level which will be examined on both a theoretical and operational level, with the indispensable recall of the fundamental principles and legal institutes of constitutional and private law governing the field. In addition, the course intends to let students appraise the risks related to technological innovation: in this respect, after the study of the essential grammar of criminal law and cybercrime, the class will be constantly challenged – also through the analysis of several business cases written by leading scholarships – in trying thinking critically towards today’s tensions between privacy and security, the numerous perils posed by blockchain technologies and the law and ethics of artificial intelligence systems. At the end of the course, students will be thus able:

* to thoroughly manage the rules of the General Data Protection Regulation 16/679 (GDPR), whose compliance has become a top-priority for both private and public companies around the world;
* to properly balance, from both a legal and a managerial standpoint, benefits and threats of technological innovation, which will increasingly be a fundamental skill to foster in order to firmly navigate the «industry 4.0».

***COURSE CONTENT***

Module I *–* *Private Law* (Prof. Vittorio Bachelet)

This first part of the course introduces to privacy and data protection rules within the framework of private law. The rights to privacy and the protection of personal data, as fundamental rights, will be explored against the backdrop of the European Union law, as the General Data Protection Regulation 16/679 (GDPR) largely replaced national laws, ensuring uniform rules across the EU. The module will focus, among other things, on the key characteristics of the EU data protection regime; the dual objectives of European data protection Regulation; the link between data protection and privacy in the EU legal order; the relationship between data protection and other rights or interests; the role of individual control over personal data in EU data protection law: tangible and intangible harms of data processing; the limits of individual control over personal data: the property approach.

Module II *–* *Criminal Law*(Prof. Ennio Alagia)

The second part of the course will then focus on the criminal facets related to privacy, security, and technological innovation. Specifically, after a brief introduction on the basic principles of criminal law, the module will concentrate on analyzing the criminal protection of the right of privacy and the realm of cybercrime and security. Attention will be then paid to the perils of technological innovation, exploring, among others, the risks of mass surveillance post COVID-19, the phenomenon of “outsider” trading, the new forms of algorithmic market manipulation, the legal threats of blockchain technologies and the connections between cryptocurrencies and money laundering, and the law and ethics of artificial intelligence systems. This Module will also include a ten-hour focus on the criminogenic features of digital interactions and on specific digital threats to the art and antiquities markets.

***READING LIST[[1]](#footnote-1)***

There are no mandatory textbooks for the course.

Students might find anyhow helpful hints browsing the following references.

As for Module I

Reference book:

O. Lynskey, The Foundations of EU Data Protection Law, Oxford University Press, 2015.

Other relevant publications:

M. Gömann, Book Review: The Foundations of EU Data Protection Law by Orla Lynksey (Oxford University Press, 2015), CML Rev. 2018, 304.

S.D. Warren-L.D. Brandels, The Right to Privacy, Harvard Law Review, Vol. 4, No. 5, 1890, pp. 193-220.

S. Sharma, Data Privacy GDPR Handbook, Wiley Publishing, 2020.

B. Van Alsenoy, Data Protection Law in the EU: Roles, Responsabilities and Liability, 2019,

Ch. Kuner-L.A. Bygrave-Ch. Docksey, Commentary on the EU General Data Protection Regulation, Oxford University Press, 2018.

As for Module II

Reference books:

G.P. Fletcher, Basic Principles of Criminal Law, Oxford University Press, 1998.

J. Clough, Principles of Cybercrime, 2nd ed., Cambridge University Press, 2016.

R. Abbot, The Reasonable Robot. Artificial Intelligence and the Law, Cambridge University Press, 2020.

Other relevant publications:

D. Gunkel, The Machine Question. Critical Perspective on AI, Robots, and Ethics, MIT Press, 2012.

N. Bostrom, Superintelligence. Paths, Dangers, Strategies, Oxford University Press, 2014.

G. Hallevy, Liability for Crimes Involving Artificial Intelligence Systems, Springer, 2015.

S.J. Russel, Human Compatible: Artificial Intelligence and the Problem of Control, Viking Press, 2019.

Interpol – United Nations Interregional Crime and Justice Research Institute, Artificial Intelligence and Robotics for Law Enforcement, March 2019.

Interpol – United Nations Interregional Crime and Justice Research Institute, Towards Responsible AI Innovation. Second Interpol-Unicri Report on Artificial Intelligence for Law Enforcement, May 2020.

European Commission’s High-Level Expert Group on Artificial Intelligence, Ethics Guidelines for Trustworthy AI, April 2019.

European Commission, White Paper on Artificial Intelligence – A European approach to excellence and trust, February 2020.

M.D. Dubber – F. Pasquale – S. Das, The Oxford Handbook of Ethics and AI, Oxford University Press, 2020

Details on the readings for the specific subjects are provided in the Syllabus, whilst the course study materials will be published on the area of Blackboard reserved for students enrolled in the course.

***TEACHING METHOD***

The modules will be delivered by means of interactive frontal lectures with discussion of case studies. To succeed in the exam, attendance it is thus strongly recommended.

***ASSESSMENT METHOD AND CRITERIA***

Students must obtain the pass mark (*sufficienza*)in the end-of-course oral exam to qualify in this course. Attendance and class participation will also receive particular attention.

A separate assessment for each module is envisaged: the final grade will be the average score of the two parts. Specific instructions will be provided at the beginning of each module.

***NOTES AND PREREQUISITES***

Further information can be found on the lecturers’ webpages at *http://docenti.unicatt.it*, or on the Faculty notice board.

It is advisable to have followed a course in private law before taking this course.

In case the current Covid-19 health emergency does not allow frontal teaching, remote teaching will be carried out following procedures that will be promptly notified to students.

1. I testi indicati nella bibliografia sono acquistabili presso le librerie di Ateneo; è possibile acquistarli anche presso altri rivenditori. [↑](#footnote-ref-1)