Technology and Privacy

3rd Edition
Code: 170022
Category: Master
Credits: 60.00
Language: English
Start date: 20/02/2018
End date: 20/12/2018

Day and Time: ON LINE
Location: Course ON LINE
Places available: 24

Prices and discounts
Price: 2.840 €

Presentation

This master's degree is the result of several conversations held in recent years between practitioners and academics in the field of surveillance studies, all of whom highlighted the lack of available training in order to fill academic or technical positions in the field of privacy and data security.

In the realm of privacy and data protection, the emergence of a European Data Protection framework and the rapid growth of IT-enabled data surveillance and mining mean that privacy management is increasingly professionalised. Chief privacy officers, privacy managers and technologists are now commonplace across the public and private sectors. Privacy policies remain unevenly implemented, and there is a growing need and high demand for analysts and practitioners at the intersection of privacy and technology.

The current development of privacy-related policies (data protection, tapping communications, etc.) means that the privacy management of organisations is becoming increasingly important. The purpose of this master is to meet the growing need to train professionals devoted to privacy management matters in order to fill the positions created to fulfil the regulations in this field. Specifically, the Master's Degree in Technology and Privacy aims to meet the need arising from the proposed new 2015 European Data Protection Directive, which will make it compulsory for all companies with over 250 employees and all public bodies to have a Data Privacy Officer (DPO).

This master is therefore conceived as a qualification that will meet the existing short-term demands and long-term demands, given that demand will increase exponentially in the next few years.

Aims

This course is intended for those aiming to build or enhance their careers in the field of technology consultancy related to privacy matters. The main goals are:
– To train students to confidently tackle tasks in the field of privacy management and data protection, always linked to technological advances.

– To transfer the knowledge accumulated through collective work among academics and professionals in the fields of technology, law and policy.
– To train professionals in the field of privacy capable of designing and evaluating policies intended to protect the private sphere.

The specific aims include:
– To provide a full understanding of the social, ethical, legal and technological consequences of surveillance with special focus on the technical impact in terms of issues such as trust, proportionality and information access.
– To foster the skills to design privacy policies in a creative and analytical manner.
–To teach students how to identify key problems that threaten privacy and the stakeholders involved, and to evaluate the impact of policies.
– To develop the capacity to understand the basic elements of data protection measures, such as resistance to surveillance or privacy-enhancing tools.
– To give students a grounding in key concepts for the implementation of non-invasive technologies, such as Privacy by Design (PbD) or Privacy-enhancing technologies (PETs).

The master's degree also addresses the sociological, political, legal and ethical context in which privacy protection policies and technologies are developed.

Who the course is for

This course is aimed at professionals, students or scholars interested in the field of technology consultancy related to privacy issues.

Admission requirements

– Applications from candidates with backgrounds in criminology, law, sociology, computer science, economics, and political science.
– Candidates who have completed the first cycle of a degree can also apply; however approval of the Master's Coordination Committee is required.
Note: students who do not hold a previous university qualification will be entitled to obtain, under the same conditions, a certificate of attendance issued by the University of Girona Foundation: Innovation and Training.

Syllabus

Privacy and surveillance concepts I

The relationship between privacy, surveillance and data protection. History and Sociology of surveillance: the Panoptic and beyond. Surveillance dimensions (institutional, corporate, interpersonal). Social relations and values under surveillance. Resistance strategies: sousveillance and counterveillance. Privacy, security and transparency. Privacy Advocacy.

Design of secure systems

Technological audit: software, hardware and networks. Threat detection and modelling. Cryptography, anonymity and re-identification. Secure storage and authentication management. Translating societal concerns into technological solutions.

Privacy and surveillance concepts II

Digital identification technologies and Dataveillance. Identification practices and techno-social relations (STS). The economics of privacy. Technology and surveillance risks (function creep, disclosure, discrimination, etc.). The surveillance industry: actors and experts.

Tools and sectors I

This module provides a sectoral approach to privacy issues, through the lens of law enforcement, health, smart cities, banking, and more. Examining privacy in these contexts, with an empirical focus, the module also discusses 'data tools'. These tools are modes through which data is collected, treated, or through which the results of data treatments are applied. These include biometrics, databases, algorithms, and drones. By the end of this module, students will have a strong grasp of the landscape of privacy-invasive

and privacy-enhancing tools. Metadata. Behavioral marketing. Biometrics. Geolocation. Gamification. Algorithms. Data Brokers. Sensitive Data. Education.

Law, policy, and technology

The fundamentals of privacy law and policy. Data protection principles and data subjects' rights. Who does what: privacy professionals, managers, and technologists. DPAs: competences, possibilities, limitations. Tapping, hacking and controversies (NSA, etc.). The transatlantic debate. Limitations, problems and new technological developments.

Tools and sectors II

This module provides a sectoral approach to privacy issues, through the lens of law enforcement, health, smart cities, banking, and more. Examining privacy in these contexts, with an empirical focus, the module also discusses 'data tools'. These tools are modes through which data is collected, treated, or through which the results of data treatments are applied. These include biometrics, databases, algorithms, and drones. By the end of this module, students will have a strong grasp of the landscape of privacy-invasive and privacy-enhancing tools. Statistics and data mining. Internet of Things. Data Bases. Browsing. Drones. Location tracking, government surveillance, illegal activity and scams. CBRN Forensics. Journalism. Banking. Technological sovereignty: community networks.

Chief privacy officer I

This two-pronged module addresses the now well-entrenched professionalization of privacy managers in the public and private sectors. Building on the knowledge acquired in all the modules, this module gives students a grounding in (1) the policy elements of privacy and data protection such as European and international data protection frameworks and (2) the technical and managerial elements of a role – the Chief Privacy Officer – that is in growing demand. This includes learning how to undertake a privacy impact assessment (PIA) and how to engineer principles such as privacy by design (PbD) and how to set an organizational privacy program. Duties and responsibilities of privacy managers.European and international privacy and data protection frameworks.
Privacy policies in the public and private sectors and Public-Private Partnerships (PPP).Assessment of privacy risks and management of information requests.

Chief privacy officer II

This two-pronged module addresses the now well-entrenched professionalization of privacy managers in the public and private sectors. Building on the knowledge acquired in all the modules, this module gives students a grounding in (1) the policy elements of privacy and data protection such as European and international data protection frameworks and (2) the technical and managerial elements of a role – the Chief Privacy Officer – that is in growing demand. This includes learning how to undertake a privacy impact assessment (PIA) and how to engineer principles such as privacy by design (PbD) and how to set an organizational privacy program. Data management and computer security. Role of chief privacy officers and data protection officers. Implementing an organizational privacy program and strategy. Conducting a Privacy Impact Assessment (PIA). Engineering: Implementing Privacy by Design (PbD, PETs).

Measuring privacy and technology impacts

PIAs, SIAs, DPIAs, etc. The policy cycle: problem definition, design, implementation, evaluation and indicators. Stakeholders and value transfers: public authorities, private actors, media and civil society. Responsible research and innovation and ethics. Research project assessment and case studies.

Master's degree final project

The programme must be completed through the writing of a research paper, which takes the form of a final research project, and involves presenting a proposal beforehand.

Qualification

Master in Technology and Privacy at the University of Girona*

* Does not include shipping rates title.

Note: students who do not hold a previous university qualification will be entitled to obtain, under the same conditions, a certificate of attendance issued by the Fundació UdG: Innovació i Formació.

Teaching and Assessment

Combination of teaching material based on audio-visual tools (5 hours of material per credit), in addition to mandatory and recommended readings. A participatory approach in the form of the "learning by doing" model will be adopted both for autonomous and lecturer-led work. All students must deliver a project of study or research paper addressing one or several of the issues dealt with in the master's degree from an innovative and relevant perspective.

Evaluation system

– The basic assessment methodology is based on individual or group assignments.

– It is mandatory to deliver one practical assignment per Module. Depending on the lecturer, other assessment tests will take place during the course.

– It is mandatory to attend all the classroom-based sessions and deliver 100% of the assignments and activities for assessment in order to obtain the master's degree.

- It is mandatory to deliver a final dissertation to end the master's programme.

Financing

Bank financing

Enrolled students can pay in installments.*

The Fundació has agreements in place offering preferential terms for their students with the following entities:

– Sabadell Consumer
– CaixaBank
– Banco Santander

* Only applicable to persons resident in Spain and upon acceptance by the bank.

Teaching table

Management
Gemma Galdon Clavell
PhD in Public Policy.

Coordination
Alejandro Vélez Salas
PhD in Humanities.

Teaching staff
Gertjan Boulet
PhD candidate in Law at Faculty of Law & Criminology of Vrije Universiteit Brussel.

Augusto Délkader
Political scientist and public sector consultant.

Claudia Diaz
PhD Assistant Professor at the COSIC research group of the Department of Electrical Engineering (ESAT) at the KU Leuven.

Hervé Falciani
Systems Engineer, whistle-blower and creator of the Falciani list, providing information on 130,000 suspected tax evaders with Swiss bank accounts.

Francesco Flammini
PhD, IEEE Senior Member and ACM Distinguished Speaker.

Gemma Galdon Clavell
PhD in Public Policy.

Antonella Galetta
PhD researcher, Vrije Universiteit Brussel.

Gloria González Fuster
PhD in Law.

Josian Llorente
Cultural manager.

Genís Margarit
Telecom engineer and IT security consultant.

Lisa Lucile Owens
PhD candidate and Paul F. Lazarsfeld Fellow at Columbia University, New York.

José Manuel Pérez Marzabal
Master of Laws, PhD candidate.

Xosé Quiroga
Bachelor of Laws, journalist.

Elvira Santiago
Postdoctoral researcher.

Katarzyna Szymielewicz
Lawyer specialised in human rights and technology, co-founder and President of the Panoptykon Foundation.

Jacqui Taylor

PhD, web scientist.

Mario Viola
PhD in Law.

*Management reserves the right to modify the teaching staff, if necessary, to ensure the levels of quality and professional category.

Promoting entities
Fundació UdG: Innovació i Formació

Eticas Foundation