Cybersecurity, legislazione e gestione della sicurezza

PARTE I - INFORMAZIONI GENERALI

Tipologia di corso

Master

Titolo del corso

Cybersecurity, legislazione e gestione della sicurezza

PARTE II - REGOLAMENTO DIDATTICO ORGANIZZATIVO

Indirizzo web del corso

https://giurisprudenza.uniroma3.it/didattica/post-lauream

Il Corso di Studio in breve

Il Master universitario di primo livello in "Master in cybersecurity, legislazione e gestione della sicurezza" propone una formazione specialistica post lauream sul tema della sicurezza cibernetica. Nello specifico, l'obiettivo è quello di far acquisire adeguati strumenti metodologici e competenze, teoriche e pratiche a chi, nel settore pubblico o privato, deve essere in grado di affrontare le sfide poste dalle nuove tecnologie, per comprendere, definire e risolvere questioni in tema di sicurezza cibernetica. La proposta didattica si fonda sull'interdisciplinarietà dei saperi, a fronte della eterogeneità delle conoscenze indispensabili per la prevenzione di eventuali situazioni di crisi, per la gestione di eventuali attacchi informatici, per il monitoraggio dei flussi economico-finanziari, per il contrasto al cybercrime. Il Corso si articolerà in due parti. La prima, dal taglio teorico, sarà connotata dall'attività di docenza e seminariale, organizzate dal Dipartimento di Giurisprudenza e da quello di Ingegneria di Roma Tre, per analizzare questioni giuridiche, sotto diversi profili - sovranazionali, penalistici, pubblicistici, amministrativistici, di diritto industriale e di management-aziendale – e per approfondire le più delicate questioni relative agli algoritmi, ai sistemi informativi, all'internet delle cose, alle infrastrutture critiche e alla loro sicurezza. La seconda parte del corso, invece, avrà un taglio eminentemente pratico-operativo, per mezzo del coinvolgimento nell'attività di docenza di esperti della Guardia di Finanza, per l'esame delle questioni in materia economico-finanziaria, relative al contrasto al riciclaggio e al finanziamento del terrorismo e della Polizia postale, per lo studio dei modelli teorici e delle prassi operative in tema di investigazione proattiva in rete, di contrasto al cybercrime, al cyberterrorismo, in tema di digital forensics. Si mira altresì a sviluppare competenze avanzate sul diritto delle nuove tecnologie e sul bilanciamento tra protezione delle banche dati e tutela dei diritti, con un focus sulle problematiche di più stringente attualità, relative al crescente potere dei c.d. attori del capitalismo della sorveglianza e al rapporto tra sovranità statale e digitale. Il Corso vuole offrire un bagaglio di strumenti indispensabili per la specializzazione nel campo della cybersecurity di funzionari e dirigenti delle Pubbliche Amministrazioni, di operatori delle Forze dell'ordine, di operatori nell'ambito della sicurezza economico-finanziaria o del settore bancario e creditizio, di esperti di crimini informatici, di professionisti e consulenti, in considerazione della sempre maggiore importanza della figura del Chief Information Security Officer (CISO) nell'organigramma aziendale

Obiettivi formativi specifici

Il percorso formativo e# in grado di assicurare una preparazione adeguata sia dal punto di vista del quadro teorico di riferimento, che delle conoscenze pratico-applicative in materia di cybersecurity, al fine di specializzare operatori delle forze dell'ordine, professionisti e consulenti, esperti in crimini informatici, avvocati e funzionari amministrativi nel campo della cybersicurezza, nonché i futuri Chief Information Security Officer (CISO).Lo scopo del Master e# quello di fornire gli strumenti adeguati a implementare le conoscenze dei partecipanti, tanto da un punto di vista teorico, quanto pratico-operativo, tenuto conto dell'apporto che in tal senso sarà fornito dalla Guardia di Finanza e dalla Polizia postale, al fine di offrire una formazione che consenta di affrontare le sfide, anche professionali, del settore della cybersecurity nella realtà contemporanea, ove ai rischi tradizionali si aggiungono le numerose e sempre crescenti minacce cyber, con evidenti ripercussioni sul rapporto tra i diversi poteri e sulla tutela dei diritti fondamentali.

Informazioni utili agli studenti

-

Descrizione modalità di svolgimento

Possono essere ammessi al Master, in qualità di uditori, soggetti non in possesso del diploma di laurea, per venire incontro alle esigenze di numerose figure professionali che si misurano quotidianamente con problemi relativi alla cybersecurity, ma che non hanno conseguito il titolo necessario all'iscrizione al Master. Tali uditori – selezionati anch'essi in base al curriculum vitae – potranno partecipare alle lezioni e alle attività didattiche organizzate nell'ambito del Master, senza sostenere le prove di verifica e la prova finale. Al termine verrà consegnato loro un attestato di partecipazione, senza riconoscimento di crediti formativi. Agli uditori si riconosce la riduzione del 25% della quota di iscrizione all'intero Master

Requisiti di ammissione

- Scadenza delle domande di ammissione: Domande di ammissione entro il 10 gennaio 2025. Iscrizione entro il 20 gennaio 2025. - Classi di laurea dei titoli di accesso e ogni altro requisito specifico: Laurea triennale, magistrale, specialistica o titolo di studio equipollente in Giurisprudenza, Scienze politiche, Economia, Ingegneria. In presenza di posti disponibili, si valuteranno, ai fini della ammissione, lauree conseguite presso Dipartimenti diversi da quelli sopra indicati, sulla base del percorso formativo dell'interessato. - Criteri di selezione nel caso in cui le domande di ammissione superino il numero massimo di ammessi: Curriculum vitae ed eventuale colloquio. - Procedure e criteri per il riconoscimento di crediti maturati dagli studenti nel corso degli studi universitari precedenti ai fini di una eventuale riduzione del percorso formativo e delle tasse d'iscrizione: Nessuno.

Numero di posti

50

Durata prevista

1 Anno

Crediti previsti

60

Lingua di insegnamento

ITA

Modalità didattica

PrevalentementeDistanza

Tasse di iscrizione ed eventuali esoneri

https://www.uniroma3.it/didattica/post-lauream/

La tassa d'iscrizione all'intero Corso di Master è stabilita in Euro 2.500,00 (Euro 2.000 per i soggetti che beneficiano della Convenzione PA 110 e lode), da versare in due rate: la prima con scadenza 20 gennaio 2025 e la seconda con scadenza il 31 maggio 2025.
All'importo della prima rata sono aggiunti l'imposta fissa di bollo e il contributo per il rilascio del diploma o dell'attestato.
Le quote di iscrizione non sono rimborsate in caso di volontaria rinuncia, ovvero in caso di non perfezionamento della documentazione prevista per l'iscrizione al Corso.
Tassa di iscrizione per gli appartenenti a tutte le Forze dell'Ordine: Euro 1.500.

Esonero dalle tasse di iscrizione
Coloro i quali si trovino in condizioni di disabilità, con riconoscimento di handicap ai sensi dell'articolo 3, commi 1 e 3, della legge 5 febbraio 1992, n. 104, o con un'invalidità pari o superiore al 66% sono tenuti in ogni caso al pagamento della prima rata di iscrizione al Corso.
Per usufruire dell'esonero è necessario allegare alla domanda di ammissione un certificato di invalidità rilasciato dalla struttura sanitaria competente indicante la percentuale riconosciuta.

Tassa di iscrizione per uditori
La tassa di iscrizione ai Corsi in qualità di uditori è fissata in Euro 1875.

Rilascio titolo congiunto

Titolo normale

Direttore del Corso

Pistorio Giovanna

ROMA TRE
UNIVERSITÀ DEGLI STUDI

PIANO DELLE ATTIVITA' FORMATIVE

(Insegnamenti, Seminari di studio e di ricerca, Stage, Prova finale)

Anno	Denominazione	SSD	CFU	Ore	Tipo Att.	Lingua
1	**20110826 - Attacchi informatici e sistemi di protezione**	IUS/17	3	15	I	ITA
1	**20110828 - Crimini informatici e indagini forense**	IUS/16	5	25	I	ITA
1	**20110824 - Cybercrime: modelli teorici e prassi operative**	IUS/17	1	5	I	ITA
1	**20110823 - Cybersecurity e cybercrime**	IUS/17	1	5	I	ITA
1	**20110813 - Cybersecurity e Data Management**	IUS/01	2	10	I	ITA
1	**20110816 - Cybersecurity e nuove tecnologie. Profili informatici**	ING-INF/05	6	30	I	ITA
1	**20110825 - Cybersecurity, cybercrime, cyberterrorismo**	IUS/17	3	15	I	ITA
1	**20110812 - Cyberspazio e diritto internazionale**	IUS/13	2	10	I	ITA
1	**20110834 - Il comparto della sicurezza**	IUS/09	4	20	I	ITA
1	**20110827 - L'utilizzo dell'IA nella cybersecurity e nel cybercrime**	IUS/17	2	10	I	ITA
1	**20110833 - La normativa antiriciclaggio**	SECS-P/09	4	20	I	ITA
1	**20110814 - La tutela penale della sicurezza informatica**	IUS/17	2	10	I	ITA
1	**20110815 - Nuovi poteri e diritti fondamentali nel Cyberspazio**	IUS/09	2	10	I	ITA
1	**20110811 - Sicurezza e Cybersecurity nell'Unione europea**	IUS/14	2	10	I	ITA
1	**20110829 - Tutela della spesa pubblica**	IUS/05	4	20	I	ITA
1	**20110830 - Tutela delle entrate**	IUS/05	4	20	I	ITA

OBIETTIVI FORMATIVI

20110826 - Attacchi informatici e sistemi di protezione

Italiano

A partire da un inquadramento giuridico, nazionale e sovranazionale, in tema di cybercrime, i moduli 1/6 mirano a esaminare, sul piano normativo e casistico, le questioni di più stringente attualità relative alla cybersecurity, con particolare riferimento all'attività investigativa svolta in rete. L'ampia disponibilità di strumenti tecnologici, materiali e virtuali ha consentito infatti lo sviluppo di nuove forme di criminalità, caratterizzate da un crescente ricorso alle nuove tecnologie e identificabili come cybercrime. È in tale contesto che assumono particolare rilievo la conoscenza del quadro normativo, interno e sovranazionale, i modelli teorici e le prassi operative, sia sul piano preventivo che sanzionatorio.

Inglese

Beginning with a legal framework, both national and supranational, on the subject of cybercrime, Modules 1/6 aim to examine, on a normative and casuistic level, the most pressing current issues related to cybersecurity, with particular reference to the investigative activity carried out online. Indeed, the wide availability of technological, material and virtual tools has enabled the development of new forms of crime, characterized by an increasing use of new technologies and identifiable as cybercrime. It is in this context that knowledge of the regulatory framework, both domestic and supranational, theoretical models and operational practices, both at the preventive and sanctioning levels, assume particular importance.

20110828 - Crimini informatici e indagini forense

Italiano

A partire da un inquadramento giuridico, nazionale e sovranazionale, in tema di cybercrime, i moduli 1/6 mirano a esaminare, sul piano normativo e casistico, le questioni di più stringente attualità relative alla cybersecurity, con particolare riferimento all'attività investigativa svolta in rete. L'ampia disponibilità di strumenti tecnologici, materiali e virtuali ha consentito infatti lo sviluppo di nuove forme di criminalità, caratterizzate da un crescente ricorso alle nuove tecnologie e identificabili come cybercrime. È in tale contesto che assumono particolare rilievo la conoscenza del quadro normativo, interno e sovranazionale, i modelli teorici e le prassi operative, sia sul piano preventivo che sanzionatorio.

Inglese

Beginning with a legal framework, both national and supranational, on the subject of cybercrime, Modules 1/6 aim to examine, on a normative and casuistic level, the most pressing current issues related to cybersecurity, with particular reference to the investigative activity carried out online. Indeed, the wide availability of technological, material and virtual tools has enabled the development of new forms of crime, characterized by an increasing use of new technologies and identifiable as cybercrime. It is in this context that knowledge of the regulatory framework, both domestic and supranational, theoretical models and operational practices, both at the preventive and sanctioning levels, assume particular importance.

20110824 - Cybercrime: modelli teorici e prassi operative

Italiano

A partire da un inquadramento giuridico, nazionale e sovranazionale, in tema di cybercrime, i moduli 1/6 mirano a esaminare, sul piano normativo e casistico, le questioni di più stringente attualità relative alla cybersecurity, con particolare riferimento all'attività investigativa svolta in rete. L'ampia disponibilità di strumenti tecnologici, materiali e virtuali ha consentito infatti lo sviluppo di nuove forme di criminalità, caratterizzate da un crescente ricorso alle nuove tecnologie e identificabili come cybercrime. È in tale contesto che assumono particolare rilievo la conoscenza del quadro normativo, interno e sovranazionale, i modelli teorici e le prassi operative, sia sul piano preventivo che sanzionatorio.

Inglese

Beginning with a legal framework, both national and supranational, on the subject of cybercrime, Modules 1/6 aim to examine, on a normative and casuistic level, the most pressing current issues related to cybersecurity, with particular reference to the investigative activity carried out online. Indeed, the wide availability of technological, material and virtual tools has enabled the development of new forms of crime, characterized by an increasing use of new technologies and identifiable as cybercrime. It is in this context that knowledge of the regulatory framework, both domestic and supranational, theoretical models and operational practices, both at the preventive and sanctioning levels, assume particular importance.

20110823 - Cybersecurity e cybercrime

Italiano

A partire da un inquadramento giuridico, nazionale e sovranazionale, in tema di cybercrime, i moduli 1/6 mirano a esaminare, sul piano normativo e casistico, le questioni di più stringente attualità relative alla cybersecurity, con

particolare riferimento all'attività investigativa svolta in rete. L'ampia disponibilità di strumenti tecnologici, materiali e virtuali ha consentito infatti lo sviluppo di nuove forme di criminalità, caratterizzate da un crescente ricorso alle nuove tecnologie e identificabili come cybercrime. È in tale contesto che assumono particolare rilievo la conoscenza del quadro normativo, interno e sovranazionale, i modelli teorici e le prassi operative, sia sul piano preventivo che sanzionatorio.

Inglese

Beginning with a legal framework, both national and supranational, on the subject of cybercrime, Modules 1/6 aim to examine, on a normative and casuistic level, the most pressing current issues related to cybersecurity, with particular reference to the investigative activity carried out online. Indeed, the wide availability of technological, material and virtual tools has enabled the development of new forms of crime, characterized by an increasing use of new technologies and identifiable as cybercrime. It is in this context that knowledge of the regulatory framework, both domestic and supranational, theoretical models and operational practices, both at the preventive and sanctioning levels, assume particular importance.

20110813 - Cybersecurity e Data Management

Italiano

Il modulo 3 è volto ad analizzare le problematiche relative alla gestione del rischio digitale, nelle sue molteplici dimensioni, tenuto conto dell'esigenza di tutela dei dati, dei sistemi e delle reti aziendali.

Inglese

Module 3 is aimed at analyzing issues related to digital risk management in its many dimensions, taking into account the need to protect corporate data, systems and networks.

20110816 - Cybersecurity e nuove tecnologie. Profili informatici

Italiano

Il modulo mira a fornire conoscenze informatiche, di carattere generale, indispensabili per la risoluzione delle problematiche in tema di sicurezza informatica, intelligenza artificiale, internet delle cose, infrastrutture critiche.

Inglese

The module aims to provide IT knowledge, of a general nature, which is essential for solving problems in cybersecurity, artificial intelligence, the Internet of Things, and critical infrastructure.

20110825 - Cybersecurity, cybercrime, cyberterrorismo

Italiano

A partire da un inquadramento giuridico, nazionale e sovranazionale, in tema di cybercrime, i moduli 1/6 mirano a esaminare, sul piano normativo e casistico, le questioni di più stringente attualità relative alla cybersecurity, con particolare riferimento all'attività investigativa svolta in rete. L'ampia disponibilità di strumenti tecnologici, materiali e virtuali ha consentito infatti lo sviluppo di nuove forme di criminalità, caratterizzate da un crescente ricorso alle nuove tecnologie e identificabili come cybercrime. È in tale contesto che assumono particolare rilievo la conoscenza del quadro normativo, interno e sovranazionale, i modelli teorici e le prassi operative, sia sul piano preventivo che sanzionatorio.

Inglese

Beginning with a legal framework, both national and supranational, on the subject of cybercrime, Modules 1/6 aim to examine, on a normative and casuistic level, the most pressing current issues related to cybersecurity, with particular reference to the investigative activity carried out online. Indeed, the wide availability of technological, material and virtual tools has enabled the development of new forms of crime, characterized by an increasing use of new technologies and identifiable as cybercrime. It is in this context that knowledge of the regulatory framework, both domestic and supranational, theoretical models and operational practices, both at the preventive and sanctioning levels, assume particular importance.

20110812 - Cyberspazio e diritto internazionale

Italiano

Il modulo 2 è volto ad approfondire il ruolo dell'ordinamento internazionale nella disciplina del cyberspazio, tenuto conto delle problematiche legate alla c.d. governance di internet. Attraverso l'esame di casi concreti, relativi ad attacchi informatici, sarà poi possibile comprendere il rapporto tra poteri pubblici e privati, il ruolo della sovranità statale e il regime di responsabilità nel cyberspazio.

Inglese

Module 2 is aimed at exploring the role of the international legal system in regulating cyberspace, taking into account

issues related to so-called Internet governance. Through the examination of concrete cases, related to cyber attacks, it will then be possible to understand the relationship between public and private powers, the role of state sovereignty and the liability regime in cyberspace.

20110834 - Il comparto della sicurezza

Italiano

In un'ottica di sicurezza economico-finanziaria, il modulo 7 mira ad approfondire le problematiche relative alla tutela della spesa pubblica, da un punto di vista normativo, amministrativo e istituzionale. Oggetto di importante approfondimento è il rapporto di collaborazione tra i vari attori istituzionali coinvolti nel processo volto al miglioramento dell'efficienza e dell'efficacia economico-finanziaria del Paese. Il modulo 8 è volto invece a esaminare le attività nazionali ed internazionali di contrasto alle frodi fiscali. Il modulo 9 mira ad analizzare il quadro normativo sulla sicurezza dei mercati finanziari, al fine di illustrare le misure di prevenzione e sanzionatorie antiriciclaggio. Nell'ambito del modulo 10, tenuto conto del complesso quadro normativo interno e sovranazionale, saranno approfondite le problematiche della sicurezza in mare, con particolare attenzione al problema dell'immigrazione irregolare.

Inglese

From the perspective of economic-financial security, Module 7 aims to explore issues related to the protection of public spending, from regulatory, administrative and institutional perspectives. The subject of important study is the cooperative relationship between the various institutional actors involved in the process aimed at improving the country's economic-financial efficiency and effectiveness. Module 8, on the other hand, is aimed at examining domestic and international activities to combat tax fraud. Module 9 aims to analyze the regulatory framework on financial market security in order to illustrate anti-money laundering prevention and sanction measures. Within Module 10, taking into account the complex domestic and supranational regulatory framework, the issues of security at sea will be explored in depth, with particular attention to the problem of irregular migration.

20110827 - L'utilizzo dell'IA nella cybersecurity e nel cybercrime

Italiano

A partire da un inquadramento giuridico, nazionale e sovranazionale, in tema di cybercrime, i moduli 1/6 mirano a esaminare, sul piano normativo e casistico, le questioni di più stringente attualità relative alla cybersecurity, con particolare riferimento all'attività investigativa svolta in rete. L'ampia disponibilità di strumenti tecnologici, materiali e virtuali ha consentito infatti lo sviluppo di nuove forme di criminalità, caratterizzate da un crescente ricorso alle nuove tecnologie e identificabili come cybercrime. È in tale contesto che assumono particolare rilievo la conoscenza del quadro normativo, interno e sovranazionale, i modelli teorici e le prassi operative, sia sul piano preventivo che sanzionatorio.

Inglese

Beginning with a legal framework, both national and supranational, on the subject of cybercrime, Modules 1/6 aim to examine, on a normative and casuistic level, the most pressing current issues related to cybersecurity, with particular reference to the investigative activity carried out online. Indeed, the wide availability of technological, material and virtual tools has enabled the development of new forms of crime, characterized by an increasing use of new technologies and identifiable as cybercrime. It is in this context that knowledge of the regulatory framework, both domestic and supranational, theoretical models and operational practices, both at the preventive and sanctioning levels, assume particular importance.

20110833 - La normativa antiriciclaggio

Italiano

In un'ottica di sicurezza economico-finanziaria, il modulo 7 mira ad approfondire le problematiche relative alla tutela della spesa pubblica, da un punto di vista normativo, amministrativo e istituzionale. Oggetto di importante approfondimento è il rapporto di collaborazione tra i vari attori istituzionali coinvolti nel processo volto al miglioramento dell'efficienza e dell'efficacia economico-finanziaria del Paese. Il modulo 8 è volto invece a esaminare le attività nazionali ed internazionali di contrasto alle frodi fiscali. Il modulo 9 mira ad analizzare il quadro normativo sulla sicurezza dei mercati finanziari, al fine di illustrare le misure di prevenzione e sanzionatorie antiriciclaggio. Nell'ambito del modulo 10, tenuto conto del complesso quadro normativo interno e sovranazionale, saranno approfondite le problematiche della sicurezza in mare, con particolare attenzione al problema dell'immigrazione irregolare.

Inglese

From the perspective of economic-financial security, Module 7 aims to explore issues related to the protection of public spending, from regulatory, administrative and institutional perspectives. The subject of important study is the cooperative relationship between the various institutional actors involved in the process aimed at improving the country's economic-financial efficiency and effectiveness. Module 8, on the other hand, is aimed at examining domestic and international activities to combat tax fraud. Module 9 aims to analyze the regulatory framework on financial market security in order to illustrate anti-money laundering prevention and sanction measures. Within Module 10, taking into account the complex domestic and supranational regulatory framework, the issues of security at sea will be explored in

depth, with particular attention to the problem of irregular migration.

20110814 - La tutela penale della sicurezza informatica

Italiano

Il modulo 4 mira a esaminare le questioni di natura penale che riguardano il rapporto tra cybersecurity e reati informatici. Le questioni di più stringente attualità ruotano attorno a valutazioni ad ampio spettro che non si limitano a interventi di natura esclusivamente repressiva, tramite l'inasprimento delle pene per i reati informatici, l'introduzione di nuove figure di reato e di aggravanti specifiche, ma prevedono attività di natura educativa, preventiva e promozionale.

Inglese

Module 4 aims to examine the criminal issues surrounding the relationship between cybersecurity and cybercrimes. The most pressing issues revolve around wide-ranging evaluations that are not limited to interventions of an exclusively repressive nature, through the tightening of penalties for cybercrimes, the introduction of new crime figures and specific aggravating factors, but involve activities of an educational, preventive and promotional nature.

20110815 - Nuovi poteri e diritti fondamentali nel Cyberspazio

Italiano

Il modulo 5 è volto a esaminare l'incidenza della cybersecurity, nelle sue poliedriche prospettive, sull'assetto costituzionale e, in particolare, sul rapporto tra poteri e sulla tutela dei diritti. A fronte della crescente incidenza di intrusioni informatiche da parte di gruppi hacker in apparenza privati ma alle volte etero-diretti da poteri pubblici, si dimostra l'emersione di dispositivi ibridi di minaccia pubblico/privata. La risposta, in questo caso, diviene di necessità essa stessa ibrida, attraverso forme di partenariato strategico tra attori istituzionali pubblici e soggetti privati. Questa ultima prospettiva sottolinea la rilevanza dei grandi player internazionali del digitale, i quali, autentici poteri privati, finiscono per divenire essenziali ai fini della stessa conservazione della sovranità statale. Di contro, la loro preponderanza sugli apparati statali segnala i rischi di cattura da parte della sfera privata delle amministrazioni pubbliche e soprattutto di apprensione dei dati personali. Attraverso l'esame di casi concreti, si mira a fornire agli iscritti al Master un quadro esauriente per comprendere anche i rischi legati al ruolo ormai decisivo degli attori del c.d. capitalismo della sorveglianza sulle funzioni dei pubblici poteri e sulla salvaguardia dei diritti fondamentali

Inglese

Module 5 is aimed at examining the impact of cybersecurity, in its multifaceted perspectives, on constitutional arrangements and, in particular, on the relationship between powers and the protection of rights. In the face of the growing incidence of cyber intrusions by hacker groups ostensibly private but sometimes hetero-directed by public powers, the emergence of hybrid public/private threat devices is demonstrated. The response, in this case, becomes of necessity itself hybrid, through forms of strategic partnership between public institutional actors and private entities. This latter perspective underscores the relevance of large international digital players, which, authentic private powers, end up becoming essential to the very preservation of state sovereignty. Conversely, their preponderance over state apparatuses signals the risks of capture by the private sphere of government and especially the apprehension of personal data. Through the examination of concrete cases, we aim to provide Master's students with a comprehensive framework for understanding also the risks associated with the now decisive role of the actors of so-called surveillance capitalism on the functions of public authorities and the safeguarding of fundamental rights

20110811 - Sicurezza e Cybersecurity nell'Unione europea

Italiano

Il modulo 1 mira a fornire un'introduzione di carattere generale sul ruolo della sicurezza e della cybersecurity in ambito europeo, tenuto conto, in particolare, del complesso ed eterogeneo quadro normativo e delle problematiche applicazioni giurisprudenziali, tenuto conto delle ricadute sugli Stati e sui singoli cittadini. Seguendo la linea concettuale evolutiva della Corte di Giustizia, dalle sentenze Breyer e e Tele2 Sverige c. Watson fino alla sentenza C-154/21, e quella, parimenti articolata, dei testi normativi come le Direttive NIS, NIS2 e il recentemente approvato Regolamento AI Act, verranno messi in evidenza i punti di forza e di potenziale debolezza dell'approccio euro-unitario alla sicurezza digitale.

Inglese

Module 1 aims to provide a general introduction to the role of security and cybersecurity in the European context, taking into account, in particular, the complex and heterogeneous regulatory framework and problematic case law applications, given the impact on states and individual citizens. Following the evolving conceptual line of the Court of Justice, from the Breyer and and Tele2 Sverige v. Watson to the C-154/21 ruling, and that, equally articulated, of regulatory texts such as the NIS Directives, NIS2 and the recently passed AI Act Regulation, the strengths and potential weaknesses of the Euro-Union approach to digital security will be highlighted.

20110829 - Tutela della spesa pubblica

Italiano

In un’ottica di sicurezza economico-finanziaria, il modulo 7 mira ad approfondire le problematiche relative alla tutela della spesa pubblica, da un punto di vista normativo, amministrativo e istituzionale. Oggetto di importante approfondimento è il rapporto di collaborazione tra i vari attori istituzionali coinvolti nel processo volto al miglioramento dell’efficienza e dell’efficacia economico-finanziaria del Paese. Il modulo 8 è volto invece a esaminare le attività nazionali ed internazionali di contrasto alle frodi fiscali. Il modulo 9 mira ad analizzare il quadro normativo sulla sicurezza dei mercati finanziari, al fine di illustrare le misure di prevenzione e sanzionatorie antiriciclaggio. Nell’ambito del modulo 10, tenuto conto del complesso quadro normativo interno e sovranazionale, saranno approfondite le problematiche della sicurezza in mare, con particolare attenzione al problema dell’immigrazione irregolare.

Inglese

From the perspective of economic-financial security, Module 7 aims to explore issues related to the protection of public spending, from regulatory, administrative and institutional perspectives. The subject of important study is the cooperative relationship between the various institutional actors involved in the process aimed at improving the country's economic-financial efficiency and effectiveness. Module 8, on the other hand, is aimed at examining domestic and international activities to combat tax fraud. Module 9 aims to analyze the regulatory framework on financial market security in order to illustrate anti-money laundering prevention and sanction measures. Within Module 10, taking into account the complex domestic and supranational regulatory framework, the issues of security at sea will be explored in depth, with particular attention to the problem of irregular migration.

20110830 - Tutela delle entrate

Italiano

In un’ottica di sicurezza economico-finanziaria, il modulo 7 mira ad approfondire le problematiche relative alla tutela della spesa pubblica, da un punto di vista normativo, amministrativo e istituzionale. Oggetto di importante approfondimento è il rapporto di collaborazione tra i vari attori istituzionali coinvolti nel processo volto al miglioramento dell’efficienza e dell’efficacia economico-finanziaria del Paese. Il modulo 8 è volto invece a esaminare le attività nazionali ed internazionali di contrasto alle frodi fiscali. Il modulo 9 mira ad analizzare il quadro normativo sulla sicurezza dei mercati finanziari, al fine di illustrare le misure di prevenzione e sanzionatorie antiriciclaggio. Nell’ambito del modulo 10, tenuto conto del complesso quadro normativo interno e sovranazionale, saranno approfondite le problematiche della sicurezza in mare, con particolare attenzione al problema dell’immigrazione irregolare.

Inglese

From the perspective of economic-financial security, Module 7 aims to explore issues related to the protection of public spending, from regulatory, administrative and institutional perspectives. The subject of important study is the cooperative relationship between the various institutional actors involved in the process aimed at improving the country's economic-financial efficiency and effectiveness. Module 8, on the other hand, is aimed at examining domestic and international activities to combat tax fraud. Module 9 aims to analyze the regulatory framework on financial market security in order to illustrate anti-money laundering prevention and sanction measures. Within Module 10, taking into account the complex domestic and supranational regulatory framework, the issues of security at sea will be explored in depth, with particular attention to the problem of irregular migration.