

WEB SERIES

COLLANA DI SCIENZE E STRATEGIE DEL DIGITALE  
I CAMPI, LO SVILUPPO, I MERCATI

7

*Direttore*

Elisabetta ZUANELLI  
Università degli Studi di Roma "Tor Vergata"

*Comitato scientifico*

Roberto BASILI  
Nicola BLEFARI MELAZZI  
Giuseppe BIANCHI  
Giovanni CREA  
Università Europea di Roma  
Claudio FRANCHINI  
Giorgio LENER  
Francesco RULLI  
Franco SALVATORI  
Antonio SANFILIPPO  
Qatar Foundation, Qeeri

*Comitato redazionale*

Mirto Silvio BUSICO  
Consulente ICT  
Paolo POMATI  
Università degli Studi del Piemonte Orientale Amedeo Avogadro  
Saverio RUBINI  
Ingegnere elettronico, funzionario informatico della Pubblica Amministrazione

I membri del Comitato scientifico e del Comitato redazionale senza affiliazione sono da intendersi afferenti all'Università degli Studi di Roma "Tor Vergata".

## WEB SERIES

COLLANA DI SCIENZE E STRATEGIE DEL DIGITALE  
I CAMPI, LO SVILUPPO, I MERCATI



Conoscere le nuove visioni multidisciplinari dell'innovazione digitale: i campi, lo sviluppo, i mercati.

L'innovazione digitale oggi è trasversale a tutte le discipline e i mondi del sapere e del fare: dal diritto all'economia, dalla salute all'ambiente, dai beni culturali al territorio, dalle discipline artistiche allo spettacolo.

In questo periodo storico gli addetti ai lavori dell'intero panorama tecnologico sono chiamati a confrontarsi con temi e sfide prospettiche. I temi riguardano i servizi digitali ipermediali inediti in Internet: libri, giochi, film, musica; servizi immobiliari, turistici, bancari, assicurativi e finanziari; informazione giornalistica, piattaforme social relazionali, professionali e scientifiche. Le sfide, invece, riguardano: "Internet delle cose" per la casa, l'azienda, la città, la persona; reti potenti, *big data analyzing*, motori di ricerca, *crawler*, applicativi vari su dispositivi fissi e mobili; regolazione di Internet e *cloud*, mercato digitale unico aperto, *cybersecurity* e *cybercrime*.

Questo universo digitale esploso è solo l'inizio di una rivoluzione globale e di nuove visioni, nella ricerca e nello sviluppo, nei mercati e nelle società "connesse", che stanno modificando i nostri stili di vita.



# ***Cybersecurity, protezione dei dati, privacy***

Temi, nozioni, applicazioni. Un approccio interdisciplinare

*a cura di*

**Elisabetta Zuanelli**

*Contributi di*

Riccardo Abeti, Danilo Benedetti, Mirto Silvio Busico  
Antonio Capobianco, Maria Cristina Cataudella, Emanuela Cerrato  
Claudio Cilli, Giovanni Crea, Cristiano Cupelli, Fabio Di Resta  
Vincenzo Farina, Domenico Faucegna, Antonino Fazio, Laura Ferola  
Fabrizio Fico, Rita Forsi, Salvatore Gagliano, Ivo Hristov, Giorgio Lener  
Raffaele Lener, Daniela Lo Monaco, Sandro Mari, Nadia Martini  
Silvano Mazzantini, Leonardo Nobile, Roberto Calogero Pellitteri  
Roberto Randazzo, Giovanni Reccia, Paola Rocco, Saverio Rubini  
Federico Santi, Federica Silvestrini, Alessandra Toma  
Bruno Valensise, Corrado Aaron Visaggio, Elisabetta Zuanelli





Aracne editrice

[www.aracneeditrice.it](http://www.aracneeditrice.it)

Copyright © MMXX  
Gioacchino Onorati editore S.r.l. – unipersonale

[www.gioacchinoonoratieditore.it](http://www.gioacchinoonoratieditore.it)  
[info@gioacchinoonoratieditore.it](mailto:info@gioacchinoonoratieditore.it)

via Vittorio Veneto, 20  
00020 Canterano (RM)  
(06) 45551463

ISBN 978-88-255-3817-5

*I diritti di traduzione, di memorizzazione elettronica,  
di riproduzione e di adattamento anche parziale,  
con qualsiasi mezzo, sono riservati per tutti i Paesi.*

*Non sono assolutamente consentite le fotocopie  
senza il permesso scritto dell'Editore.*

I edizione: dicembre 2020

# Indice

- 19 Prefazione  
*Maria Cristina Cataudella*
- 21 Presentazione  
*Giorgio Lener, Elisabetta Zuanelli*
- 25 Introduzione  
*Elisabetta Zuanelli*

## Parte I Analisi di contesto

- 31 1.1. Sicurezza economica, sicurezza nazionale e *golden power*  
*Bruno Valensise*
- 1.1.1. Il contesto economico normativo della sicurezza e la *golden power*, 32
- 45 1.2. *Cybersecurity*, protezione dei dati, *privacy*. Il contesto e gli aspetti concettuali, terminologici, operativi  
*Elisabetta Zuanelli*
- 1.2.1. Le transazioni *online* e la gestione di sistemi *online*: ruoli, minacce, vulnerabilità, attacchi, 47 – 1.2.2. Le difese, gli *antimalware* e gli antivirus, 50 – 1.2.3. Le previsioni delle aziende e il mercato della *cybersecurity*, 52 – 1.2.4. Un rapido sguardo alla sicurezza nazionale e internazionale: USA, UE, NATO, Italia, 53
- 59 1.3. Le norme. NIS, GDPR, d.l. 105/2019, *Cyber Act*  
*Elisabetta Zuanelli*
- 1.3.1. Il contesto delle norme in materia, 60 – 1.3.2. La situazione nazionale, 61

– 1.3.3. La Direttiva NIS, 61 – 1.3.4. Il GDPR e la protezione dei dati personali: trattamento, soggetti implicati, obblighi, sanzioni, 67 – 1.3.5. Il Decreto Legge 105/2019 e le norme di contesto Artt. 1,2,3,4, 69 – 1.3.6. Il *Cyber Act*, 71

73    1.4. Il Codice dell'Amministrazione Digitale (CAD)  
*Federica Silvestrini*

1.4.1. L'evoluzione del CAD, 73 – 1.4.2. I concetti e i principi, 75 – 1.4.3. Il documento, la firma, la riservatezza, 77 – 1.4.4. Art. 51: la sicurezza informatica, 80

83    1.5. I sistemi informatici. *Hardware*, *software* e reti  
*Saverio Rubini*

1.5.1. Ambiti operativi di intervento, 84 – 1.5.2. Informatica e *computer*, 85 – 1.5.3. *Software*, 87 – 1.5.4. *Bit*, *byte* e codifica, 88 – 1.5.5. *Computer* e 'non *computer*': *mobile*, *appliance*, IoT, domotica, 89 – 1.5.6. Tipi di memorie, 91 – 1.5.7. Periferiche, 92 – 1.5.8. Porte di collegamento, 93 – 1.5.9. Canali di comunicazione senza fili, 94 – 1.5.10. Canali di comunicazione attraverso linee telefoniche, 94 – 1.5.11. Reti di *computer*, 95 – 1.5.12. Internet, TCP/IP e sue caratteristiche, 96 – 1.5.13. Dispositivi e *appliance* per la Rete, 98 – 1.5.14. Siti *web* e altri servizi di comunicazione avanzata, 99 – 1.5.15. URL e domini, 101 – 1.5.16. Il DNS, 102

## Parte II

### La componente giuridico–normativa della protezione dei dati, della *privacy* e della *cybersecurity*

107    2.1. La protezione dei dati personali. Regole e pratiche nei diversi settori alla luce del decreto legislativo n. 101/2018  
*Laura Ferola*

2.1.1. Introduzione: il quadro normativo in generale, 108 – 2.1.2. Informazioni da fornire agli interessati, 109 – 2.1.3. Presupposti legittimanti il trattamento dei dati personali. Dati comuni e disciplina del consenso, con specifico riferimento ai minori. Dati 'sensibili' e dati 'giudiziari', 111

117    2.2. Principi e disposizioni fondamentali riguardanti il trattamento di dati personali in ambito pubblicistico  
*Laura Ferola*

Trattamenti per motivi di interesse pubblico, 118 – Misure di garanzia e disciplina transitoria per le autorizzazioni generali, 120 – Regole deontologiche, codici di condotta e la disciplina transitoria nei diversi settori, 123 – Brevi cenni sull'attività del Garante per la protezione dei dati personali nell'ambito dell'EDPB, 124

- 129 2.3. Organizzazione del trattamento dei dati personali  
Giovanni Crea
- 2.3.1. figure soggettive nel trattamento dei dati personali, 130 – Gestione e coordinamento del trattamento dei dati personali, 136 – 2.3.3. Il modello “titolare–responsabile”: criteri di adozione e contenuti dell’accordo, 137
- 141 2.4. Applicazione del GDPR  
Nadia Martini
- 2.4.1. I principi del GDPR: il principio di *accountability* e le sue prove, 144 – 2.4.2. L’*assessment* come *audit* sulla *privacy*: metodologie e tecniche di svolgimento, 145 – 2.4.3. Le misure tecniche e organizzative, 147
- 153 2.5. La realizzazione di alcuni strumenti di *accountability* e procedure previsti dal GDPR  
Giovanni Crea
- 2.5.1. Il principio di *accountability*, 154 – 2.5.2. Il registro delle attività di trattamento, 156 – 2.5.3. La procedura di gestione delle violazioni dei dati personali, 162
- 169 2.6. Il nuovo codice europeo delle comunicazioni elettroniche. Contratti e nuovi strumenti di regolazione dei mercati *wholesale* e *retail*  
Domenico Fauceglia
- 2.6.1. Il mercato delle comunicazioni elettroniche, 171 – 2.6.2. Il potere regolamentare *ex ante* ed *ex post*, 172 – 2.6.3. I contratti di utenza telefonica, 173
- 181 2.7. La vigilanza sui mercati finanziari  
Raffaele Lener
- 2.7.1. I mercati di riferimento, 182 – 2.7.2. I modelli, 183 – 2.7.3. La scelta del modello ibrido, 184 – 2.7.4. Il modello sovranazionale, 185 – 2.7.5. L’Unione bancaria, 187 – 2.7.6. Banche, 188 – 2.7.7. Imprese di investimento, 189 – 2.7.8. Imprese di assicurazione, 192
- 195 2.8. Il sistema di intermediazione finanziaria  
Vincenzo Farina
- 2.8.1. Definizione e funzioni del sistema finanziario, 196 – 2.8.2. Il concetto di saldo finanziario e i circuiti di copertura del fabbisogno finanziario: intermediari vs mercati finanziari, 196 – 2.8.3. La funzione creditizia delle banche, 200 – 2.8.4. La funzione monetaria delle banche e il sistema dei pagamenti, 201 – 2.8.5. Gli

*information security risk*, 201

205      2.9. Punti di contatto fra diritto penale e protezione dei dati personali

*Cristiano Cupelli, Fabrizio Fico*

2.9.1. I risvolti penalistici del Regolamento UE 2016/679 e la problematica del *ne bis in idem*, 206 – 2.9.2. Modello di organizzazione, gestione e controllo *ex d.lgs. n. 231/2001* e misure di contenimento del rischio in ambito protezione dati personali, 208 – 2.9.3. DPO e ODV. Interferenze e profili differenziali, 210 – 2.9.4. Il trattamento illecito di dati e le nuove fattispecie previste all'interno del Codice *privacy*. Gli articoli 167, 167-bis e 167-ter, 212

217      2.10. Il quadro normativo in materia di robotica e intelligenza artificiale

*Silvano Mazzantini*

2.10.1. Robotica e intelligenza artificiale: nozione, riferimenti normativi e concettuali, 219 – 2.10.2. La questione etica, l'affidabilità e il ruolo della *cybersecurity*, 222 – 2.10.3. Situazioni giuridiche e perimetro della responsabilità, 224 – 2.10.4. Intelligenza artificiale, robotica e Pubblica Amministrazione, 226

229      2.11. La tutela della salute, il Sistema Sanitario Nazionale e la protezione dei dati personali

*Riccardo Abeti*

2.11.1. Contesto, 229 – 2.11.2. Il quadro normativo e regolamentare, 230 – 2.11.3. Provvedimenti dell'Autorità Garante, 236 – 2.11.4. Altri documenti e Linee di indirizzo, 238 – 2.11.5. Il Servizio Sanitario, 240 – 2.11.6. Approccio di metodo, 241 – 2.11.7. Conclusioni, 245

247      2.12. La *privacy* nel settore bancario e nel settore assicurativo. La distribuzione dei compiti e delle responsabilità nelle organizzazioni complesse

*Fabio Di Resta*

2.12.1. I soggetti passivi degli obblighi: il titolare, i contitolari, i responsabili del trattamento e le persone autorizzate, 248 – 2.12.2. Distribuzione dei compiti e delle responsabilità in base al regolamento europeo (c.d. GDPR), 252 – 2.12.3. Un approccio pratico per individuare i responsabili e gli autonomi titolari: fornitori, consulenti e la rete di intermediari in ambito bancario e assicurativo, 255

- 259 2.13. La *privacy* nel settore bancario e assicurativo. Le frodi telematiche in ambito bancario e la tutela risarcitoria del correntista vittima di *cybercrime*  
Fabio Di Resta
- 2.13.1. Introduzione, 261 – 2.13.2. Analisi di quadro normativo: normativa sui servizi di pagamento, 262 – 2.13.3. La tutela risarcitoria del correntista nell'evoluzione della giurisprudenza dal 2009 ad oggi, 264 – 2.13.4. La tutela del correntista vittima di *SIM swap fraud*: analisi del *leading case* del Tribunale di Roma, 266 – Riferimenti bibliografici, 271
- 273 2.14. Prevenire *cyber*-rischi, difendersi e rimediare a *cyber*-attacchi. La protezione dei dati negli studi professionali  
Saverio Rubini
- 2.14.1. Attività informatiche negli studi legali e professionali, 274 – 2.14.2. Obiettivi della sicurezza informatica, 275 – 2.14.3. Attacchi fisici, 276 – 2.14.4. Identità digitali, credenziali e *password*, 277 – 2.14.5. CIE, CNS, TS e PIN, OTP, SPID, 278 – 2.14.6. Tipi di programmi applicativi, 279 – 2.14.7. Diritti di utilizzo dei programmi, 280 – 2.14.8. Dati, banche dati, informazioni, documenti e *file*, 281 – 2.14.9. Protezione dati riservati nei documenti informatici, 282 – 2.14.10. Protezione dati riservati in Windows 10 e con i *browser*, 283 – 2.14.11. Strumenti *software* di protezione, 284 – 2.14.12. Antivirus e *firewall*, 285 – 2.14.13. Perdita di dati e loro recupero, 287 – 2.14.14. *Rescue disk*, 287 – 2.14.15. Copie e repliche, 288 – 2.14.16. Copie di salvataggio (*backup*) e ripristino (*restore*), 289

### Parte III

## La componente gestionale-aziendalistica della protezione dei dati, della *privacy* e della *cybersecurity*

- 295 3.1. La *governance* della sicurezza. La visione gestionale/organizzativa  
Leonardo Nobile
- 3.1.1. Il punto di partenza, 296 – 3.1.2. *Governance* vs gestione, 298 – 3.1.3. La *governance* della sicurezza, 300 – 3.1.4. Processi di sicurezza, 301 – 3.1.5. Strutture organizzative di sicurezza, 302 – 3.1.6. Flussi di informazioni e *item* informativi, 303 – 3.1.7. Persone, *skill* e competenze, 303 – 3.1.8. Principi, *policy* e procedure, 304 – 3.1.9. Cultura, etica e comportamento, 305 – 3.1.10. Servizi, infrastrutture e applicazioni, 306
- 307 3.2. Trasformazione digitale e *cybersecurity*  
Federico Santi
- 3.2.1. Dalla fase di digitalizzazione dei processi tradizionali alla fase dei processi

- digitali *by design*, 308 – 3.2.2. L'ambiente digitale trasformato: l'esplosione dei *device*, delle utenze e dei dati verso architetture iper-distribuite e *asset* immateriali, 309 – 3.2.3. Le ragioni dell'incremento della rilevanza della *cybersecurity*, 311 – 3.2.4. La *security & privacy by design*, 313 – 3.2.5. L'IoT. Dall'ICS/SCADA all'IP-zzazione: opportunità e rischi, 314 – 3.2.6. *Next generation security*, 316 – 3.2.7. I trend 2020–2021, 317 – 3.2.8. La centralità del dato e della sua protezione, 318
- 321    3.3. Requisiti minimi per la gestione della *cybersecurity* e della protezione dei dati nella PA  
*Saverio Rubini*
- 3.3.1. Misure minime per la PA, 322 – 3.3.2. Implementazione delle misure minime per la PA, 323
- 327    3.4. Metodi, tecniche e tecnologie per il *risk assessment* e la *risk evaluation*  
*Roberto Randazzo*
- 3.4.1. Requisiti di valutazione e trattamento del rischio contenuti nella ISO/IEC 27001:2013, ISO/IEC 20000-1:2018 e ISO 22301:2019, 328 – 3.4.2. Processo di gestione del rischio, 330
- 335    3.5. Rischio *cyber* nel settore finanziario e rilevanza sistemica  
*Emanuela Cerrato, Antonino Fazio, Daniela Lo Monaco, Roberto Calogero Pellitteri*
- 3.5.1. Il sistema finanziario: caratteristiche e potenziali vulnerabilità sistemiche, 335 – 3.5.2. Rischio *cyber* e stabilità finanziaria, 337 – 3.5.3. Sfide per le autorità e risposte di *policy*, 339
- 341    3.6. La gestione dell'*Information Technology* attraverso la IT Balanced Scorecard (BSC)  
*Ivo Hristov*
- 3.6.1. Contesto di analisi, 342 – 3.6.2. Creazione di valore e crescita dell'azienda moderna, 343 – 3.6.3. La IT BSC quale strumento di allineamento e miglioramento delle *performance*, 345 – 3.6.4. Costruzione di una mappa strategica IT: l'allineamento strategico, 346 – 3.6.5. L'implementazione della BSC IT, 348 – 3.6.6. Considerazioni conclusive, 350
- 353    3.7. Principi, *tool* e *framework* a disposizione del *board* delle organizzazioni per pianificare e controllare il rischio *cyber*  
*Leonardo Nobile*
- 3.7.1. Le esigenze, 354 – 3.7.2. Gli strumenti forniti dal rapporto, 356 – 3.7.3. I 10 principi, 357 – 3.7.4. La *check list* proposta, 358 – 3.7.5. Il *framework* per il *cyber*

- risk, 363.
- 367 3.8. I fattori chiave legali e contrattuali nella gestione dei servizi IT/*outsourcing*  
Nadia Martini
- 3.8.1. Introduzione normativa GDPR e NIS e obblighi principali, 369 – 3.8.2. I fattori chiave legali e contrattuali nella gestione dei servizi IT/*outsourcing*, 371 – 3.8.3. Le coperture assicurative *cyber risk* per la *privacy* e *data protection*, 376
- 379 3.9. La *cybersecurity* nel *mobile*  
Alessandra Toma
- 3.9.1. Tutela e autotutela dell'identità *online* (lato cliente e lato organizzazione), 381 – 3.9.2. *Mobile app monitoring and assessment* (ricerca *market* in cui sono pubblicate le app, censimento, rimozione, monitoraggi di sicurezza minacce e vulnerabilità, tecniche di analisi statica e dinamica delle app), 383 – 3.9.3. *Mobile app security by design*, 385
- 389 3.10. Le funzioni e i *task* CERT/CSIRT  
Elisabetta Zuanelli
- 3.10.1. Le difese operative: le squadre tecniche CERT e CSIRT, 389 – 3.10.2. La tipologia di CERT, 392 – 3.10.3. I *task* CSIRT e le classificazioni ENISA, 394 – 3.10.4. Attività e ruoli organizzativi nella *cybersecurity*, 397
- 399 3.11. Gli standard utilizzati per la sicurezza delle informazioni e la certificazione del sistema di gestione. Requisiti e linee guida  
Roberto Randazzo
- 3.11.1. Contenuti della ISO/IEC 27001:2013, 400 – 3.11.2. Struttura della norma, 401.
- 415 3.12. La gestione dei servizi IT, famiglia delle norme ISO 20000, la norma ISO 20000-1:18. Requisiti *focus*, principi chiave e buone pratiche  
Roberto Randazzo
- 3.12.1. Contenuti della ISO/IEC 20000-1:2018, 416 – 3.12.2. Struttura della norma, 418

- 425    3.13. La continuità operativa  
      *Roberto Randazzo*

3.13.1. Contenuti della ISO 22301:2019, 426 – 3.13.2. Struttura della norma, 428

- 437    3.14. Gli obblighi per le infrastrutture critiche nazionali ed europee  
      *Danilo Benedetti*

3.14.1. Le infrastrutture critiche, 438 – 3.14.2. Genesi e struttura della direttiva NIS, 439 – 3.14.3. Elementi normati dalla direttiva NIS, 440 – 3.14.4. Sicurezza dei sistemi ICS/SCADA, 443

## Parte IV

### La componente tecnologico–digitale della protezione dei dati, della *privacy* e della *cybersecurity*

- 449    4.1. *Open source* e sicurezza  
      *Mirto Silvio Busico*

4.1.1. Concetti di base sulla sicurezza, 450 – 4.1.2. Cos'è l'*open source*, 452 – 4.1.3. Cos'è Linux, 456 – 4.1.4. Servizi *open source* per la produttività individuale, 457

- 459    4.2. Servizi *open source* per i centri di calcolo  
      *Mirto Silvio Busico*

4.2.1. Reti, *firewall* e gestione della rete, 460 – 4.2.2. Tipi di *server*, 463 – 4.2.3. *Server* della posta, 466 – 4.2.4. *Database* e gestione dei dati, 467 – 4.2.5. Virtualizzazione e *cloud*, 467 – 4.2.6. Il progresso dall'*hardware* al *cloud*, 469 – 4.2.7. Il progresso del *software*: dal monolite ai *microservice*, 472

- 475    4.3. Il *malware*: tipologie e *payload*; attacchi informatici, attaccanti e strumenti di difesa  
      *Saverio Rubini*

4.3.1. Il *malware*, 476 – 4.3.2. Virus e categorie di virus, 477 – 4.3.3. I troiani, 478 – 4.3.4. I *worm*, 478 – 4.3.5. I *ransomware*, 480 – 4.3.6. I *rootkit*, 480 – 4.3.7. *Spyware* e *adware*, 481 – 4.3.8. Altri oggetti informatici legati al *malware*, 482 – 4.3.9. Tipologie di attaccanti, 483 – 4.3.10. Ingegneria sociale, 485 – 4.3.11. *Spam*, 486 – 4.3.12. *Phishing*, 487 – 4.3.13. Attacchi e danni APT, 488

- 491 4.4. *Malware analysis*  
Corrado Aaron Visaggio
- 4.4.1. L'identificazione del *malware*, 491 – 4.4.2. Calcolo dell'*hash*, 494 – 4.4.3. Trovare le stringhe, 494 – 4.4.4. Il formato *Portable Executable*, 495 – 4.4.5. *Sandbox*, 497 – 4.4.6. *Process Monitor*, 498 – 4.4.7. *IdaPro*, 498
- 501 4.5. Indicatori di compromissione e tecniche di evasione  
Corrado Aaron Visaggio
- 4.5.1. *CybOx*, 502 – 4.5.2. *STIX*, 505 – 4.5.3. *TAXII*, 506 – 4.5.4. *Yara*, 507 – 4.5.5. *Sandbox*, 508 – 4.5.6. Tecniche di evasione dei *malware*, 509
- 511 4.6. *Cybersecurity analytics*: classificazioni, tassonomie, ontologie  
Elisabetta Zuanelli
- 4.6.1. L'ecosistema della sicurezza *cyber*-informatica e la *big data analytics* per la *cybersecurity*, 512 – 4.6.2. Modelli di tassonomie e ontologie della *cybersecurity*: la prospettiva internazionale, 514 – 4.6.3. La piattaforma ontologica *cybersecurity* Pragmema POC: architettura e struttura, 523
- 533 4.7. Il processo di *incident response*  
Antonio Capobianco
- 4.7.1. Introduzione, 534 – 4.7.2. Il processo di *incident response* secondo NIST, 535 – 4.7.3. *Incident response cycle*, 535
- 547 4.8. La *kill chain* come processo di *incident response*  
Antonio Capobianco
- 4.8.1. I passaggi della *kill chain*, 548 – 4.8.2. Esempio di attacco con analisi *kill chain*, 553 – 4.8.3. Attacco a *Target*, 554
- 559 4.9. Analisi tecnologica della *resilience in cloud*  
Danilo Benedetti
- 4.9.1. Introduzione: la corsa alle nuvole, 560 – 4.9.2. I modelli di *delivery* nel *cloud*, 561 – 4.9.3. Il governo del *cloud*, 564 – 4.9.4. Aspetti tecnologici della sicurezza delle operazioni 'fra le nuvole', 567 – 4.9.5. *Cloud Access Security Broker* (CASB), 573 – 4.9.6. Cenni alla *Cloud Controls Matrix*, 575 – 4.9.7. Certificazioni specifiche, 576

- 577    4.10. *Covert channel* & steganografia  
Claudio Cilli
- 4.10.1. Introduzione, 578 – 4.10.3. Steganografia, 580 – 4.10.4. Applicazioni, 584 – 4.10.5. Contromisure, 586 – I *covert channel* sono semplici da realizzare e usare?, 587 – 4.10.6. Conclusioni, 589

- 595    4.11. Progettazione di soluzioni per la raccolta e il monitoraggio degli eventi  
Paola Rocco
- 4.11.1. Il contesto, 596 – 4.11.2. Funzionalità di *security*, *information* ed *event management*, 598 – 4.11.3. Architettura di un SIEM, 603

## Parte V Prospettive istituzionali

- 611    5.1. Il Nucleo Speciale Tutela *Privacy* e Frodi Tecnologiche della Guardia di finanza: *dark web*, *privacy* e *digital forensics*  
Giovanni Reccia
- 5.1.1. Il Nucleo Speciale Tutela *Privacy* e Frodi Tecnologiche della Guardia di finanza, 611 – 5.1.2. Il *dark web*, 613 – 5.1.3. *Privacy* e *accountability*, 616 – 5.1.4. La prova digitale, 618
- 621    5.2. Il CVCN nel contesto del dl. n. 105/2019  
Sandro Mari
- 5.2.1. Ricostruzione della normativa che istituisce il CVCN, 622 – 5.2.2. Compiti ed attività del CVCN, 622 – 5.2.3. Posizionamento del CVCN rispetto agli schemi di certificazione e valutazione esistenti, 624
- 627    5.3. Accordi internazionali e standard/*framework* di sicurezza (evoluzione normativa e compiti istituzionali in materia di protezione di settori e infrastrutture strategiche e di certificazione di sicurezza informatica)  
Rita Forsi
- 5.3.1. Contesto, 628 – 5.3.2. La Direttiva NIS: una svolta decisiva, 631 – 5.3.3. Il recepimento della direttiva NIS in Italia, 634 – 5.3.4. Sicurezza e integrità delle reti di comunicazione elettronica, 636 – 5.3.5. Il 5G, 638 – 5.3.6. Il *Cyber Act*, 639 – 5.3.7. Il perimetro di sicurezza nazionale cibernetica, 641

643 5.4. Il mondo della Difesa e il *cyberspace*. Cultura operativa e *best practice* a supporto del *decision making*  
Salvatore Gagliano

5.4.1. Il mondo della Difesa e le sue peculiarità, 644 – 5.4.2. Analisi della minaccia, 646 – 5.4.3. Quadro normativo di riferimento e scenario NATO, 648 – 5.4.4. Il Comando per le Operazioni in Rete (C.O.R.), 651



## Prefazione

MARIA CRISTINA CATAUDELLA\*

Scrivo questa breve prefazione, in qualità di Direttore del Dipartimento di Management e Diritto della Facoltà di Economia dell'Università degli Studi di Roma "Tor Vergata", con particolare piacere e apprezzamento. Da tempo, infatti, il Dipartimento si pone l'obiettivo di realizzare percorsi formativi improntati al contributo di discipline diverse nell'ambito dell'economia moderna.

Il contesto nel quale l'opera si colloca è quello dell'*economia digitale*, preconizzata nelle dinamiche storiche della *new economy* a partire dagli anni '90 del secolo scorso, specificamente improntate alla nozione di *net economy*. La rete delle reti, Internet, ha rivoluzionato il nostro modo di lavorare, studiare, relazionarci attraverso nuovi dispositivi, servizi digitali, piattaforme abilitanti. Le nuove finestre della ricerca e dello sviluppo richiedono una sempre maggiore integrazione, culturale prima che tecnologica, come sollecita oggi l'Unione europea nell'accelerazione prevista dei processi di digitalizzazione.

La sfida nell'ambito della trasformazione digitale, vera e propria rivoluzione economica in corso, si è concretizzata nel terzo millennio in un riposizionamento delle società a tecnologia avanzata che si confrontano con le velocissime innovazioni proposte dai giganti globali delle tecnologie digitali in Rete.

Al beneficio straordinario cui si correla oggi l'apporto dell'intelligenza artificiale, delle reti 5g, delle infrastrutture gestionali delle piattaforme *cloud* corrisponde oggi, tuttavia, la controfaccia negativa di un'economia digitale criminale che si alimenta di dati, utilizzati a scopi malevoli. È la dimensione globale delle minacce cibernetiche che preoccupa in maniera crescente nell'uso confidente delle nuove tecnologie che devono essere improntate alla *cybersecurity* e alla protezione dei dati, confrontandosi con il particolare rischio di esposizione dannosa nelle infrastrutture critiche. Energia, finanza, sanità, ambiente, trasporti, sociale rischiano di diventare ambiti di razzia e di danno socioeconomico crescente.

\* Professore ordinario di Diritto del lavoro presso l'Università degli Studi di Roma "Tor Vergata".

In questo contesto si colloca il Master di secondo livello in “Competenze digitali per la protezione dei dati, la *cybersecurity* e la *privacy*”, attivo nel nostro Dipartimento dall’anno accademico 2017–2018.

Nel percorso formativo, le prospettive cogenti di natura giuridico–normativa e delle relative norme si traducono nella domanda di nuove professionalità gestionali della sicurezza e della protezione dei dati, incardinate alle competenze tecnologiche strette. I tre assi formativi teorico–applicativi del Master costituiscono anche un importante passo nella direzione di una nuova cultura del digitale e dell’economia digitale stessa.

Il volume, curato da Elisabetta Zuanelli, Direttore scientifico del Master, è redatto dai docenti del master stesso e riflette la necessità di un linguaggio integrato, appunto multi — e interdisciplinare, destinato, in prima battuta, ai partecipanti al percorso formativo ma anche ad un confronto conoscitivo più ampio.

È con questo intento che proponiamo il volume ai lettori interessati, nella prospettiva di nuovi e più ampi terreni di lavoro, integrati nella comunità tecnico–scientifica dei partenariati, nella formazione come nella ricerca.