# SOMMARIO

Le responsabilità relative alle frodi telematiche bancarie: SIM Swap Fraud e class action – *Fabio Di Resta*

1. Introduzione 9
2. Le frodi telematiche e la SIM Swap Fraud 12
3. Il quadro normativo sui servizi di pagamento: l'arduo percorso per la tutela del correntista nel mercato unico digitale 17
4. Il risarcimento del danno da frodi telematiche bancarie: evoluzione storica e situazione attuale 20
5. La mancanza di un intervento normativo specifico del legislatore italiano sulla responsabilità da trattamento illecito dei dati 23
6. Analisi del *leanding case* del Tribunale di Roma sulla SIM Swap Fraud 28
7. La class action in Italia e all'estero: il necessario percorso per risarcire la "perdita di controllo dei dati" 36

Data protection e cybersecurity: per lo sviluppo di una cultura del dato e della sicurezza – *Isabella Corradini*

1. Introduzione 43
2. Persone e dati 44
3. Errore umano e comportamenti imprudenti 47
4. Atteggiamento *vs* comportamento nella protezione dei dati 50
5. L'ingegneria sociale 53
   *5.1 Principi psicologici e forme dell'ingegneria sociale* 55
6. Un nuovo "mindset" per la cybersecurity 59
7. Conclusioni 62

Direttiva NIS e Decreto attuativo – *Massimo Davi*

1. Premessa 67
2. La Direttiva: oggetto e ambito di applicazione 69
3. La strategia nazionale in materia di sicurezza della Rete e dei sistemi informativi 71
4. Il Decreto Legislativo n. 65/2018 76
5. La possibile evoluzione: dalla NIS1 alla NIS2 81

Dal Cybersecurity Act al perimetro di sicurezza nazionale cibernetico – *Mauro Alovisio*

1. Premessa 91
2. Il Cybsersecurity Act 92
   *2.1 Struttura del Cybersecurity Act* 96
3. Il Perimetro di sicurezza nazionale cibernetico 100
   *3.1 I soggetti del perimetro* 103
   *3.2 La notifica degli incidenti informatici* 110
   *3.3 Le misure di sicurezza per gli operatori del perimetro* 114
   *3.4 Adempimento delle procedure* 117
4. L'Agenzia per la cybersicurezza nazionale 123

Analisi penale dei crimini informatici nelle infrastrutture critiche – *Giovanni Grassucci*

1. Criminalità informatica: cenni storico-normativi 139
2. Reati posti a tutela dell'inviolabilità del domicilio. Art. 615-*ter* c.p. Accesso abusivo a sistema informatico 146
3. Delitti contro il patrimonio mediante frode. Art. 640-*ter* c.p. Frode informatica 153
4. Illeciti penali in ambito protezione dei dati personali 161

5. La Legge 133/2019: Cybersecurity, responsabilità penale e responsabilità degli enti 166
6. Spunti di discussione: in caso di malware di criptazione il pagamento è stato di necessità o condizione di responsabilità? 170

La tutela legale dell'utente nelle comunicazioni elettroniche: nuove sfide e prospettive di riforma – *Silvano Sacchi*

1. Introduzione 179
2. La disciplina normativa relativa alla vita privata e alle comunicazioni elettroniche nel quadro complessivo delle fonti di rango sovranazionale e nazionale 181
   *2.1 Dalla Direttiva 2002/58/CE al D.Lgs. 196/2003* 181
   *2.2 Le modifiche apportate alla Direttiva e-privacy dalle Direttive nn. 2006/24/CE e 2009/136/CE* 185
   *2.3 La dichiarazione di invalidità della Direttiva 2006/24/CE ad opera della Corte di Giustizia Europea (sentenza della Corte di Giustizia Europea – Grande Camera – dell'8 aprile 2014 sulle cause riunite C-293/12 e C-294/12)* 189
   *2.4 Regole e strumenti per il bilanciamento tra i diritti dell'utente e le esigenze di sicurezza interna degli Stati membri* 192
3. Lo stato dell'arte: tra discipline nazionali ancora in contrasto con i principi e le affermazioni della sentenza dell'8 aprile 2014 e prospettive di riforma per il superamento della Direttiva 2002/58/CE 197
4. Conclusioni 202

L'importanza della digital forensics – *Nanni Bassetti*

1. Introduzione 205
2. Digital forensics: caratteristiche e competenze necessarie 206
3. Gli ambiti d'applicazione e le fasi 209

*3.1 Le fasi* 209
4. Esempio di applicazioni della digital forensics in ambito aziendale 211
*4.1 Esempio 1* 212
*4.2 Esempio 2* 215
5. Conclusioni 223