

INDICE

	pag.
Premessa di Giovanni Ziccardi	xvii
Gli autori	xxi

Parte I

IL SETTORE LEGALE SOTTO ATTACCO INFORMATICO E LE VULNERABILITÀ TIPICHE DELLO STUDIO, DEI COLLEGHI, DEI CLIENTI E DEI FORNITORI

1.	La sicurezza informatica propria, dei clienti e dei colleghi di Giovanni Ziccardi	
1.	Un approccio iniziale corretto all'idea di <i>cybersecurity</i>	3
2.	Le regole di <i>Embroker</i> per la <i>cybersecurity</i> negli studi legali	4
3.	La necessità di dotarsi di attrezzature professionali	8
4.	La comprensione dei concetti di multiutenza, di autenticazione e di profili di autorizzazione	9
5.	L'aggiornamento costante del sistema	11
6.	La differenza tra strumenti (e applicazioni) "personali" e "professionali"	12
7.	La protezione tramite gli antivirus	13
8.	La centralità della ridondanza dei dati e del <i>backup</i>	14
9.	La cifratura dei dati e delle comunicazioni	14
10.	L'uso intelligente del <i>cloud computing</i>	15
11.	La necessità di nuovi comportamenti	15
12.	L'uso corretto della posta elettronica	16
13.	Una proposta di "piano di spesa" razionale per il professionista (che voglia dirsi) tecnologico	16
2.	Gli attacchi a studi legali nella società digitale tra realtà e <i>fiction</i> di Gabriele Suffia	
1.	I principali attacchi informatici a studi legali e avvocati negli ultimi anni	19
2.	Il caso dei <i>Panama Papers</i>	22

	pag.
3. Alcuni casi che hanno coinvolto la Cina	23
4. Il caso del <i>data breach</i> di DLA	24
5. Lo studio legale a rischio di attacchi informatici nella <i>fiction</i>	25
3. Le vulnerabilità tipiche di uno studio legale	
di Alessandro Rodolfi	
1. La protezione dei dati e della rete dello studio, dei clienti e dei colleghi	29
2. La vulnerabilità della posta elettronica e della corrispondenza	32
3. La vulnerabilità dei canali di comunicazione	36
4. La vulnerabilità dei server e dei computer	38
5. La vulnerabilità delle applicazioni	40
6. La vulnerabilità del cloud e dei dati in mobilità	41
7. La vulnerabilità del "perimetro" fisico dei dati	44
8. La vulnerabilità nelle relazioni con i fornitori	45
Parte II	
LA VULNERABILITÀ INFORMATICA CAUSATA DA COMPORTAMENTI SBAGLIATI E LA HUMAN SECURITY	
4. La <i>human security</i> e le vulnerabilità del comportamento umano	
di Giovanni Ziccardi	
1. La centralità dei comportamenti nel mondo della <i>cybersecurity</i>	49
2. L'insicurezza per "ignoranza" tecnologica od organizzativa	49
3. L'insicurezza per ingenuità	51
4. L'insicurezza per leggerezza e distrazione nei comportamenti o per cattive abitudini	51
5. L'insicurezza causata da disagio nei confronti della tecnologia	52
6. L'insicurezza del dipendente/collaboratore	53
5. La difesa dagli attacchi di <i>phishing</i> nel settore legale	
di Giulia Pesci	
1. La natura degli attacchi di <i>phishing</i>	55
2. Alcuni dati interessanti sul fenomeno	58
3. La componente psicologica sottesa agli attacchi di <i>phishing</i>	59
4. Prevenire e difendersi dal <i>phishing</i>	61
5. La casistica	65

	pag.
6. La redazione di una <i>policy</i> in tema di <i>phishing</i> di Giovanni Ziccardi	
1. Prepararsi all'attacco informatico più comune	69
2. La cultura, prima di tutto	69
3. La semantica e l'analisi del testo	70
4. Prestare attenzione al <i>phishing</i> mirato	71
5. Dedicare particolare cura alla gestione delle credenziali	72
6. Diffidare delle richieste di dati bancari e di carte di credito	72
7. Non farsi attirare dai link	73
8. Gestire in maniera diffidente tutti gli allegati	73
9. Evitare di rispondere a mittenti (s)conosciuti	73
10. Confidare nella buona azione degli antivirus	74
11. Non farsi condizionare dal senso di vergogna per l'accaduto	74
7. Proteggersi dai furti d'identità e dalle estorsioni a fini sessuali di Andrea Scirpa	
1. Dall'identità personale all'identità digitale	75
2. Il rischio del furto d'identità	76
3. Le estorsioni a fini sessuali	81
8. Formare bene chiunque tratti i dati: elaborare una prima <i>policy</i> di <i>cybersecurity</i> di Giovanni Ziccardi	
1. Premessa: il dato al centro del processo di sicurezza	85
2. La necessaria attenzione ai dati cartacei e allo smaltimento/ distruzione dei rifiuti non elettronici	85
3. Adottare particolare cura nella gestione delle credenziali e di dati identificativi e prestare attenzione ai sempre più frequenti attacchi di <i>phishing</i>	87
4. Rendere l'autenticazione a più fattori obbligatoria	87
5. Verificare in ogni momento che i profili di autorizzazione informa- tica dei dipendenti e dei collaboratori siano rigidamente correlati alle specifiche mansioni	88
6. Prestare particolare attenzione a eventuali sistemi/impianti di vi- deosorveglianza	89
7. Prestare particolare attenzione al campo "cc" delle e-mail e alla gestione degli allegati	90
8. Prestare attenzione al furto di chiavette USB, dischi esterni e computer portatili	90

	pag.
9. Prestare particolare attenzione a non mescolare dati di terzi (" <i>mix-up</i> " di dati) soprattutto in ambito contabile e sanitario	91
10. Prestare particolare attenzione a evadere con cura, e in tempi molto rapidi, qualsiasi richiesta di esercizio dei diritti che possa provenire da clienti o terzi	91
11. Limitare il più possibile l'utilizzo di strumenti pensati per un utilizzo personale, quali iCloud e WhatsApp, e prediligere strumenti di comunicazione e di <i>cloud</i> pensati per un uso sicuro e professionale .	92
12. Prestare particolare attenzione a non esporre nei locali dello studio, o in prossimità dello stesso, elenchi con dati o indirizzi che possano essere fotografati e diffusi, ad esempio, sui social network	92
13. La gestione di eventuali <i>data breach</i> e incidenti informatici deve partire dal basso, dal singolo utente, di qualsiasi profilo	93
14. Nelle realtà professionali più grandi, comprendere il ruolo del <i>Data Protection Officer</i> e la sua centralità con riferimento alla <i>cybersecurity</i>	94
15. Prestare attenzione a che non siano pubblicate, su web e riviste, notizie relative a soggetti identificabili o contenenti dati personali .	94
16. Evitare di utilizzare gruppi di indirizzi, archivi di clienti e contenuti di banche dati di cui si ha la disponibilità per finalità private o, comunque, differenti da quelle stabilite in origine	95
17. Prestare particolare attenzione nel momento in cui si trattano dati cosiddetti "sensibili"	95
18. Tenere sempre sotto controllo il proprio sistema di autenticazione e quello altrui, verificare la presenza di proprie credenziali nel deep web e aggiornare le proprie procedure di ingresso nei sistemi . .	96
19. In caso di problemi di sicurezza, prevedere tempi di reazione e di contenimento/limitazione dei danni accurati ma rapidi	97
20. Prestare particolare attenzione quando si effettuano test e riavvii di applicazioni e sistemi informativi, migrazioni di database effettuate da esperti interni ed esterni e formare con particolare cura (" <i>training</i> ") chiunque tratti i dati dello studio	98
9. Insegnare al giurista le basi della <i>cybersecurity</i> di Giovanni Ziccardi	
1. Un documento specifico sulla <i>cybersecurity</i> negli studi legali della International Bar Association.	101
2. La parte tecnologica	101
3. Le misure organizzative di <i>cybersecurity</i>	103
4. La formazione dello staff	104

	pag.
10. Il delicato rapporto tra <i>cybersecurity</i> e pandemia e tra sicurezza informatica e mobilità di Giovanni Ziccardi	
1. Come comportarsi in periodo di pandemia	105
2. La sicurezza in mobilità: il computer portatile e lo smartphone dell'avvocato	106
11. Una prima proposta/griglia di percorso di formazione per lo staff di uno studio legale (venti ore di "corso immaginario") di Giovanni Ziccardi	
1. Programmare un piano di formazione accurato per lo studio legale	109
2. Una proposta di "griglia" formativa applicabile a tutti i tipi di realtà (venti ore di formazione)	109
 Parte III	
GDPR, DATA PROTECTION E DATA GOVERNANCE NELL'ATTIVITÀ LEGALE	
12. La <i>data protection</i> nello studio professionale di Samanta Stanco	
1. Il GDPR nelle micro, piccole, medie e grandi realtà legali	115
2. La trasparenza nei confronti dei clienti	117
3. Le misure adeguate di sicurezza	118
4. Il sito web del professionista	120
5. La gestione delle newsletter legali	121
13. L'analisi e la mappatura del rischio di Alessandra Salluce	
1. L'importanza e la funzione dell'analisi del rischio	123
2. Fare un'analisi del rischio di uno studio legale	125
3. La valutazione di impatto	129
14. Il registro dei trattamenti di uno studio legale di Giulia Escurole	
1. L'importanza del registro dei trattamenti e le sue finalità	135
2. I soggetti obbligati alla redazione del registro	138

	pag.
3. Le informazioni che deve contenere il registro del titolare e il registro del responsabile del trattamento	140
4. L'aggiornamento del registro	143
5. La tenuta del registro negli studi legali di piccole e grandi dimensioni	143
15. La gestione della sicurezza dello studio professionale tramite le <i>policy</i> di Chiara Ciccia Romito	
1. Un'introduzione al tema e il processo di elaborazione di <i>policy</i> di sicurezza	151
2. Un esempio/modello di <i>policy</i> per l'uso degli strumenti informatici .	156
3. Un esempio/modello di <i>policy</i> per l'uso della posta elettronica e delle risorse di rete dello studio legale	159
4. Un esempio/modello di <i>policy</i> per la corretta gestione degli attacchi di <i>phishing</i>	161
5. Un esempio/modello di <i>social media policy</i> con riferimento alla presenza dei professionisti sui social network	163
6. Un esempio/modello di <i>policy</i> per la corretta gestione dei <i>data breach</i> nello studio legale	164
 Parte IV	
SEGRETO, CONTROLLO DEI DATI, INFORMAZIONI SU FONTI APERTE, DIFESA DAGLI ATTACCHI	
16. Segreto professionale "informatico" e deontologia di Marcello Bergonzi Perrone	
1. Il rapporto tra sicurezza dello studio e deontologia	169
2. L'aggiornamento informatico, il rapporto sicuro con i clienti e il segreto professionale digitale	174
17. OSINT e informazioni rilasciate (e ricercate) su fonti aperte di Pierluigi Perri	
1. L'idea di OSINT	181
2. Il non lasciare tracce	185
3. L'OSINT "attivo" nell'attività professionale e nella ricerca d'informazioni	190

	pag.
18. La difesa e le tecniche per sfuggire agli attacchi di Giuseppe Battaglia	
1. Avvocati e <i>cybersecurity</i>	193
2. Il <i>ransomware</i>	194
3. Lo <i>spyware</i>	200
4. Il servizio informatico in <i>outsourcing</i>	204
5. L'utilizzo degli antivirus in ambito legale	207
6. Come scegliere un buon antivirus?	208
7. La gestione dei profili di autorizzazione e la "2 Factor Authentication"	209

Parte V

PROTEGGERE UNA REALTÀ LEGALE NELL'ERA DEL *LEGAL TECH*, DELLE RETI, DEL *CLOUD* E DEI *SOCIAL NETWORK*

19. Il problema degli <i>insiders</i> e degli attacchi dall'interno di Simone Icardi	
1. Introduzione	217
2. <i>Insiders</i> : come agiscono all'interno dell'azienda	218
3. Tipologie di <i>insiders</i>	219
4. La motivazione degli <i>insiders</i>	221
5. Incidenti informatici: un po' di numeri	222
6. La risposta al problema dell' <i>insider</i>	223
7. Osservazioni e consigli pratici	225
20. La comprensione e gestione dei <i>data breach</i> in ambito legale di Giovanni Ziccardi	
1. Cosa sono i <i>data breach</i>	227
2. Come reagire ai <i>data breach</i>	228
3. Preparare una <i>policy</i> per prevenire i <i>data breach</i>	229
21. La cifratura dei dati di Gabriele Suffia	
1. L'importanza della cifratura dei dati in ambito professionale	231
2. La cifratura dei dati dei computer	232
3. La cifratura dei dati degli smartphone e dei supporti esterni	235
4. La cifratura delle comunicazioni	237
5. La mappatura dei processi	240

	pag.
22. Le analisi interne (<i>digital forensics</i>) allo studio legale	
di Pierluigi Spera	
1. La <i>forensics</i> interna per la rilevazione di comportamenti criminali .	241
2. Le competenze dell'analista forense	243
3. Le fasi dell'analisi forense	244
4. Le migliori modalità per l'acquisizione e conservazione della fonte di prova digitale	245
5. I processi di esame ed analisi dei dati	247
6. La reportistica e le relazioni	249
23. La sicurezza nei processi telematici	
di Scott Dennis Ward	
1. Introduzione	251
2. La sicurezza della Posta Elettronica Certificata	253
3. La sicurezza della firma digitale	256
24. Lo studio sicuro nell'era del <i>legal tech</i>	
di Scott Dennis Ward	
1. Introduzione	263
2. Produzione legale automatizzata (<i>Document Automation</i>)	264
3. <i>Transaction Management</i>	264
4. <i>Knowledge Management (KM)</i>	264
5. <i>Project Management</i>	265
6. Piattaforme per l'amministrazione dello studio legale o <i>Practice Management System</i>	265
7. CRM (<i>Customer Relations Management</i>)	265
8. Intelligenza artificiale (o IA)	266
9. Chi popola il mondo <i>Legal Tech</i> ?	267
10. La sicurezza nelle <i>Legal Collaboration Technology</i>	269
11. Modello di sicurezza per l'adozione di strumenti <i>Legal Tech</i>	275
25. Il professionista del diritto, lo studio legale e il <i>cloud computing</i>	
di Valerio Edoardo Vertua	
1. Introduzione	283
2. Il "computer di un altro"	285
3. Il quadro normativo	287
4. Cosa e come scegliere	290

	pag.
5. Il cloud e i device del professionista	295
6. Alcune brevi considerazioni finali	297
26. Il rischio reputazionale per l'avvocato: casistica e possibili strategie di Simone Bonavita ed Elisabetta Stringhi	
1. Il problema: il rischio reputazionale per l'avvocato	299
2. Casistica	302
3. Strategie preventive e reattive	307
4. Strategie per la prevenzione	308
5. Risposte a un incidente reputazionale	310
6. Copertura assicurativa a trasferimento del rischio	312
7. Il codice deontologico italiano ed europeo	313
8. Conclusioni	315

Parte VI

IL GIURISTA E IL MESTIERE DI *DATA PROTECTION OFFICER* (DPO): IMPOSTARE UN PERCORSO CULTURALE, FORMATIVO E TECNICO

27. Il mestiere di <i>Data protection Officer</i> e la corretta comprensione dell'attuale "mercato" dei dati e dei metadati (e dei relativi rischi) di Giovanni Ziccardi	
1. Il DPO come conoscitore dell'attuale mercato di dati e di metadati delle persone	319
2. Il DPO e la comprensione dell'importanza dei <i>big data</i>	320
3. Il DPO e la comprensione della necessità di proteggere i (meta)-dati	322
4. Il DPO e la comprensione dell'automatizzazione dell'analisi e del controllo dei dati	324
5. Paranoici vs. esibizionisti del dato	326
6. Il DPO nel mercato dei dati personali	329
7. L'esposizione in corso del nostro lato più intimo	331
8. L'intervento necessario del diritto	332
9. Le attività di profilazione segreta e i <i>data breach</i> non segnalati	333
10. La violazione dei diritti in corso	334
11. Le tecnologie come strumento di protezione	335
12. La necessità di cambiare i comportamenti	335
13. La necessaria protezione dei dati altrui	336
14. È un discorso non adatto a questi tempi?	337

	pag.
28. Il DPO e la comprensione dell'attuale società della sorveglianza e del controllo	
di Giovanni Ziccardi	
1. Il cosiddetto "neoliberalismo digitale" e le nuove forme di controllo dell'individuo	343
2. I risvolti della vicenda di Edward Snowden e del Datagate	348
3. La profilazione "selvaggia" e l'importanza del caso "Cambridge Analytica"	355
29. Il DPO e la sua necessaria formazione giuridica specifica	
di Giovanni Ziccardi	
1. Lo studio accurato del Regolamento Europeo del 2016 (GDPR) . . .	359
2. La comprensione dell'importanza dei vari adempimenti	361
3. La centralità dell'informativa e della corretta raccolta del consenso	365
4. Il ruolo del dato "personale" nell'intero sistema del GDPR	371
5. La necessaria, costante attenzione ai diritti dell'individuo	374
6. La portabilità dei dati: un nuovo, interessante diritto	377
7. La "morte" del dato come diritto fondamentale	378
8. I ruoli e le responsabilità dei vari soggetti	379
9. Il DPO: lo sceriffo che protegge i dati	380
10. L'idea di "accountability" e il nuovo approccio anglosassone . . .	383
11. Elaborare una "mappa" del trattamento dei dati	385
12. L'importanza dei dati dei minori nella società dell'informazione .	386
13. Oscurare i dati per avere sicurezza: cifratura e pseudonimizzazione	387
14. Il costante timore di una violazione dei dati	388
15. L'importanza di stabilire regole	390
16. Comprendere il nuovo quadro sanzionatorio	390
30. Il DPO e la cybersecurity (anche personale)	
di Giovanni Ziccardi	
1. Comprendere il quadro attorno al dato digitale e alla sua sicurezza	393
2. Comprendere, <i>in primis</i> , il "peso" del dato	396
3. Interpretare sempre il dato come qualcosa di "vivo"	399
4. Comprendere l'importanza di avere il dato in più "luoghi"	402
5. Comprendere i rischi connessi ai vari tipi di <i>malware</i>	404
6. Comprendere l'importanza della protezione delle credenziali . . .	407
7. L'attenzione costante ai comportamenti umani	409

	pag.
8. L'importanza di suggerire sempre la cifratura e l'oscuramento dei dati	412
9. Comprendere il ruolo delle macchine virtuali per creare ambienti sicuri	413
10. Mantenere costantemente il <i>tracking</i> ("tracciamento") delle informazioni	414
11. L'importanza di avere regole chiare iniziali circa il quadro di <i>cyber-security</i> della realtà in cui ci si trova ad operare	415
12. Comprendere l'importanza delle "migliori pratiche" da seguire nell'attività quotidiana	416
13. Avere sempre chiaro il quadro del mercato relativo a PEC, <i>cloud</i> e altri servizi sicuri per lo storage e la comunicazione dei dati	418
14. Acquisire competenze di base circa le modalità migliori per gestire gli incidenti informatici (<i>digital forensics</i>)	419
15. L'importanza che il DPO imposti e pianifichi percorsi di conoscenza e di formazione (sia propri, sia altrui)	421
16. Un'ultima considerazione: la centralità dello smartphone nel sistema attuale di governance dei dati	422
Conclusioni	425

