

# INDICE

	<i>pag.</i>
INTRODUZIONE	1
SEZIONE I OGGETTO E DELIMITAZIONE DELL'INDAGINE: L'INTELLIGENCE NELL'ERA DIGITALE E IL DIRITTO INTERNAZIONALE	
1. L'avvento dell'intelligence digitale	1
2. L'attività di intelligence e la raccolta di dati	3
3. L'intelligence in tempo di pace	5
4. Spionaggio e ciberspionaggio nel diritto internazionale	7
5. <i>La bulk collection of data</i>	9
6. Il ruolo crescente dei privati nella raccolta di informazioni	11
SEZIONE II SCOPO, METODO E PIANO DELL'INDAGINE: L'APPLICABILITÀ DEL DIRITTO INTERNAZIONALE ALLA RACCOLTA DI DATI SU VASTA SCALA NELLE RETI DIGITALI	
1. Il ciberspionaggio nel diritto internazionale consuetudinario e pattizio	13
2. La raccolta dati negli ordinamenti liberal-democratici: sorveglianza e intelligence	16
3. L'approccio metodologico	18
4. Il piano dell'indagine	19
CAPITOLO I LA RELAZIONE TRA INTELLIGENCE E DATI DIGITALI	
1. Premessa: la sinergia tra intelligence e tecnologia	23
2. Spionaggio e intelligence nell'era digitale	26

	<i>pag.</i>
3. Il ciclo e i metodi dell'intelligence: la fenomenologia della raccolta informativa	32
4. La sorveglianza strategica e l'intercettazione di dati grezzi su vasta scala	36
5. La raccolta SIGINT e la sua evoluzione. <i>La Digital Network Intelligence</i> (DNI) e l'intelligenza artificiale	39
6. <i>La Digital Network Exploitation</i> (DNE) e la <i>Computer Network Exploitation</i> (CNE)	43
7. La dimensione esterna (e interna) della SIGINT	49
8. <i>Bulk collection of data e targeted collection</i> : tra intelligence e <i>law enforcement</i>	54
9. La sovrapposizione tra le funzioni di intelligence e quelle di <i>enforcement</i> : il rapporto "Scheinin"	58
10. Oltre la sorveglianza elettronica: l'acquisizione di informazioni dal settore privato ( <i>Commercially Available Information</i> )	60

## CAPITOLO II

### LO SPIONAGGIO NEL DIRITTO INTERNAZIONALE

#### SEZIONE I

##### LO SPIONAGGIO ALLA PROVA DEL DIRITTO INTERNAZIONALE

1. Lo spionaggio e il diritto internazionale	63
2. Le tesi tradizionali sullo spionaggio nel diritto internazionale	66
3. Gli aspetti controversi nel dibattito contemporaneo in materia di spionaggio	73
4. "Al di là della sovranità": lezioni dalla sorveglianza strategica satellitare	75
5. L'intercettazione dei cavi in fibra ottica in mare o sulle coste. Le navi "spia"	80
6. Lo spionaggio nel contesto diplomatico-consolare	86
7. La sorveglianza cibernetica e gli obblighi in materia di diritti umani: cenni e rinvio	89
8. Lo spionaggio e la raccolta informativa su vasta scala nel diritto internazionale dei conflitti armati	94

#### SEZIONE II

##### L'ASCESA DELLA SORVEGLIANZA DIGITALE SU VASTA SCALA E IL DIRITTO INTERNAZIONALE

1. Premessa	100
2. L'evoluzione della sorveglianza delle comunicazioni negli USA: contesto, origini ed evoluzione	102
3. Le modalità operative dell'intelligence negli USA: <i>clandestine operations</i> e <i>covert operations</i>	106
4. ( <i>segue</i> ) Le operazioni coperte e clandestine nel cibernazio	110
5. I precursori del caso <i>Snowden</i> : i programmi <i>Echelon</i> e <i>Onyx</i>	111

	<i>pag.</i>
6. Il caso <i>Snowden</i> e la sua influenza sul piano politico e scientifico	113
7. L'azione dell'Assemblea generale delle Nazioni Unite in materia di sorveglianza	117
8. ( <i>segue</i> ) La risoluzione dell'Assemblea generale delle Nazioni Unite: <i>The right to privacy in the digital age</i>	119
9. Sintesi e prosieguo dell'indagine	121

### CAPITOLO III

## IL DIRITTO INTERNAZIONALE CONSUETUDINARIO E LA RACCOLTA DI DATI DIGITALI SU VASTA SCALA

### SEZIONE I

#### LE ATTIVITÀ DI SORVEGLIANZA

#### A FINI DI INTELLIGENCE E IL DIRITTO INTERNAZIONALE

1. Considerazioni introduttive	125
2. La sovranità e il territorio	128
3. La sovranità e il principio di non intervento negli affari interni	132
4. Lo spionaggio tra sovranità territoriale e principio di non intervento	136
5. Il concetto di "coercizione" nel principio di non intervento	144
6. Gli ambiti della sovranità e la <i>domestic jurisdiction</i>	147
7. Dalla sovranità territoriale alla sovranità digitale	149
8. L'applicabilità del diritto internazionale al cibernazio	152
9. La violazione della sovranità territoriale nelle operazioni nel cibernazio	156
10. La coercizione nel cibernazio tra "estorsione" e "controllo"	159
11. Riflessioni conclusive	163

### SEZIONE II

#### LA POSIZIONE DEGLI STATI SULL'APPLICABILITÀ DEL DIRITTO INTERNAZIONALE ALLE ATTIVITÀ CIBERNETICHE

1. Introduzione	167
2. I lavori del <i>Group of Governmental Expert</i> (GGE)	170
3. L' <i>Open-ended Working Group</i> (OEWG)	175
4. La posizione degli Stati	177
4.1. Stati Uniti	177
4.2. Regno Unito	179
4.3. Francia	182
4.4. Cina e Russia	184
4.5. Italia	187
4.6. Unione Europea	188
4.7. Sintesi	189

## SEZIONE III

LO SPIONAGGIO DIGITALE IN TEMPO DI PACE  
NEL MANUALE DI TALLINN 2.0

1. Il Manuale di Tallinn	190
2. La Regola 32 del Manuale di Tallinn 2.0	192
3. Gli attori dello spionaggio: il rapporto tra spionaggio e attività criminali nel cibernazio	196
4. Le modalità illecite dello spionaggio cibernetico: la violazione della sovranità e del principio di non intervento	198
5. Raccolta massiva di dati e sorveglianza: le implicazioni per i diritti umani e per altri settori del diritto internazionale	202
6. L'importanza e i limiti del Manuale di Tallinn	204

## CAPITOLO IV

IL CONSIGLIO D'EUROPA E LA RACCOLTA  
DI DATI DIGITALI SU VASTA SCALA

## SEZIONE I

IL CONSIGLIO D'EUROPA E LA SORVEGLIANZA DI MASSA:  
DIRITTI UMANI, *GOVERNANCE* E STRUMENTI NORMATIVI

1. Il variegato contesto del Consiglio d'Europa	207
2. I diritti umani quale limite alle attività di raccolta di dati digitali su vasta scala da parte dell'intelligence	208
3. L'azione dell'Assemblea Parlamentare dopo il 2013	209
4. <i>L'Intelligence Codex</i> e il <i>Draft Legal Instrument on Government-led Surveillance and Privacy</i>	211
5. La Commissione di Venezia e la sorveglianza strategica	212
6. Il "Rapporto sul controllo democratico ed efficace dei servizi di sicurezza nazionali"	213
7. <i>L'Intelligence Oversight Working Group</i>	214
8. La Convenzione per la protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (108) e il suo aggiornamento (108+)	216
9. Osservazioni conclusive	218

## SEZIONE II

LA SORVEGLIANZA SU VASTA SCALA NELLA GIURISPRUDENZA  
DELLA CORTE EUROPEA DEI DIRITTI DELL'UOMO

1. La CEDU e la giurisprudenza della Corte Europea dei Diritti dell'Uomo sulle intercettazioni strategiche	221
--	-----

	<i>pag.</i>
2. La sentenza <i>Klass e al. c. Germania</i> del 1978	225
2.1. Sorveglianza segreta e società democratiche	225
2.2. La legittimazione ad agire delle “vittime potenziali” e la creazione di un “quasi-giudizio” di convenzionalità in materia di intercettazioni segrete	227
2.3. Il differente orientamento della Corte suprema USA e della Corte Europea dei Diritti dell’Uomo	229
3. I criteri <i>Weber</i>	230
4. La successiva evoluzione della giurisprudenza della Corte Europea dei Diritti dell’Uomo	232
5. L’evoluzione del sistema normativo in materia di sorveglianza nel Regno Unito	234
5.1. L’influenza delle sentenze della Corte Europea dei Diritti dell’Uomo	234
5.2. I casi <i>Big Brother Watch e al. c. Regno Unito</i> e <i>Centrum för Rättvisa c. Svezia</i>	239
5.3. L’aggiornamento dei criteri <i>Weber</i> al nuovo contesto della sorveglianza su vasta scala e le <i>end-to-end safeguards</i>	245
5.4. L’attuale assetto delle intercettazioni nel Regno Unito: l’ <i>Investigatory Powers (Amendment) Act 2024</i>	248
6. L’impatto delle rivelazioni del 2013 e della giurisprudenza della Corte EDU sulla regolamentazione delle attività di intelligence in Germania	249
6.1. L’accordo tra il <i>Bundesnachrichtendienst</i> (BND), i <i>Government Communications Headquarters</i> (GCHQ), la <i>National Security Agency</i> (NSA) e l’inchiesta del <i>Bundestag</i>	249
6.2. Le sentenze del <i>Bundesverfassungsgericht</i> sul <i>BND-Gesetz</i> e sull’ <i>Artikel 10-Gesetz</i> (G 10) e il diritto internazionale	254
7. La responsabilità degli Stati nella cooperazione internazionale nelle operazioni di sorveglianza	260
8. Il <i>do ut des</i> informativo: la raccolta informativa per procura	262
9. Il ruolo della crittografia e la raccolta informativa su vasta scala	265
10. Riflessioni conclusive	269

## CAPITOLO V

### L’UNIONE EUROPEA E L’ACQUISIZIONE DI DATI DIGITALI SU VASTA SCALA

#### SEZIONE I

#### SICUREZZA NAZIONALE E INTEGRAZIONE EUROPEA: L’INTERPRETAZIONE DELL’ART. 4, PAR. 2, TUE

1. Premessa: la sicurezza nazionale degli Stati membri dell’UE e la sicurezza dell’Unione	273
---	-----

	<i>pag.</i>
2. La sicurezza nazionale tra diritto internazionale e integrazione europea	278
3. L'ambiguo ruolo dell'art. 4, par. 2, TUE: «competenza esclusiva» o «responsabilità esclusiva» degli Stati membri in materia di sicurezza nazionale?	283
4. L'eccezione dell'art. 4, par. 2, TUE sulla sicurezza nazionale da parte degli Stati membri davanti alla Corte di Giustizia	289
5. Il caso paradigmatico dell'accordo di rinegoziazione del 2015-2016 tra Regno Unito e Unione Europea e la richiesta di rafforzamento dell'art. 4, par. 2, TU	292
6. Le iniziative del Parlamento europeo: i casi <i>Echelon</i> , <i>Datagate</i> e <i>Pegasus</i>	293
7. ( <i>segue</i> ) La risposta del Regno Unito alla richiesta di audizione del direttore del GCHQ alla Commissione LIBE del Parlamento europeo in relazione al <i>Datagate</i>	297
8. La nozione di "sicurezza nazionale" nella giurisprudenza della Corte di Giustizia	299
9. Osservazioni conclusive	303

## SEZIONE II

### LA PROTEZIONE E LA CONSERVAZIONE DEI DATI PERSONALI NELLA GIURISPRUDENZA DELLA CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA

1. Premessa	306
2. Il delicato bilanciamento tra sicurezza nazionale e protezione dei dati personali nell'Unione Europea	308
3. Le tappe fondamentali del percorso normativo e giurisprudenziale in tema di protezione dei dati personali: dalla Direttiva Privacy al GDPR	310
4. La giurisprudenza successiva sulla distinzione tra conservazione e accesso ai dati	316
5. La raccolta, l'accesso e la trasmissione dei dati personali per ragioni di sicurezza nazionale nella giurisprudenza più recente della CGUE	318
6. Quale ruolo per l'art. 4, par. 2, TUE alla luce della giurisprudenza della CGUE sulla raccolta e l'accesso ai dati digitali?	322
7. La Dichiarazione OCSE sull'accesso governativo ai dati personali detenuti da entità del settore privato	325

## SEZIONE III

### IL TRASFERIMENTO DEI DATI PERSONALI NELLA GIURISPRUDENZA DELLA CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA

1. Il trasferimento e il trattamento dei dati dei passeggeri nel traffico aereo (PNR)	327
2. Il trasferimento e il trattamento dei dati finanziari tra Unione Europea e Stati Uniti	331

	<i>pag.</i>
3. Lo scambio di dati personali tra UE e USA: il <i>Safe Harbor</i> 2000	333
4. Le conseguenze dello scandalo <i>Snowden</i> nel 2013: dall'invalidazione del <i>Safe Harbor</i> all'ascesa (e caduta) del <i>Privacy Shield</i>	334
5. La nuova disciplina dei dati transatlantici successiva al 2020	336
6. La politica della privacy negli USA	337
7. ( <i>segue</i> ) Il rafforzamento delle garanzie per le attività SIGINT degli Stati Uniti e la definizione dei suoi obiettivi	339
8. Il <i>Data Privacy Framework</i> del 2023 e le garanzie comuni applicabili all'accesso governativo ai dati per scopi di sicurezza nazionale	342
9. La raccolta massiccia di dati come minaccia "straordinaria" alla sicurezza dello Stato	344
10. Dai dati personali ai dati non-personali	347
CONCLUSIONI	349
BIBLIOGRAFIA	355