



SAGGI DI DIRITTO TRIBUTARIO, AMMINISTRATIVO E DELL'ECONOMIA

Collana Tributaria

A cura di
Antonio Felice Uricchio, Gennaro Terracciano, Francesco Fimmanò

Sergio Ricchitelli – Nicola BarbuZZi

LE INTERCETTAZIONI DI CONVERSAZIONI E COMUNICAZIONI Anche a mezzo trojan dopo la riforma Bonafede

- ✓ Indice
- ✓ *Il trojan horse* e la riforma orlando:
affinamento delle tecniche investigative e captatori informatici
- ✓ Gli Assetti organizzativi e gestionali della riforma
- ✓ Comunicazioni di servizio di appartenenti al dipartimento delle informazioni per la sicurezza e ai servizi di informazione per la sicurezza



Sommario

CAPITOLO PRIMO

L'EVOLUZIONE NORMATIVA DEL SISTEMA DELLE INTERCETTAZIONI. DALLA PRIMA GUERRA MONDIALE ALLA TRATTATIVA STATO MAFIA. (IL PARADIGMA DIACRONICO)

1	LA GENESI STORICA DEL SISTEMA DELLE INTERCETTAZIONI NELLA PRIMA GUERRA MONDIALE: GIOLITTI, AURIO CARLETTI E IL SERVIZIO INTERCETTAZIONI..... »	19
2	IL VENTENNIO FASCISTA E LA SECONDA GUERRA MONDIALE..... »	24
	1) L'istituzione del servizio d'ascolto: Ugo Guspini. L'OVRA, il Codice Rocco e lo scoppio della Seconda guerra mondiale.....	24
3	IL PRIMO PERIODO REPUBBLICANO »	29
	1) Dalla Carta costituzionale alla Legge 9 aprile 1974, n. 98.....	29
4	GLI ANNI DI PIOMBO, TRA EVERSIONE, TERRORISMO E CRIMINALITÀ ORGANIZZATA: LA LEGGE N. 191 DEL 18 MAGGIO 1978..... »	33
5	DAL MODELLO INQUISITORIO A QUELLO ACCUSATORIO: LE INTERCETTAZIONI NEL NUOVO CODICE DI PROCEDURA PENALE »	37
6	LE INTERCETTAZIONI E LA LEGISLAZIONE DI CONTRASTO AL TERRORISMO INTERNAZIONALE..... »	43
	1) La Legge 23 dicembre 1993 n. 547.....	43
	2) L'attentato alle Torri Gemelle e la lotta al terrorismo: le Leggi 15 dicembre 2001 n. 438 e 31 luglio 2005 n. 155.....	43
7	LA LEGISLAZIONE DELLA SECONDA REPUBBLICA E IL NUOVO MILLENNIO. IL LODO MACCANICO-SCHIFANI, IL PROCESSO TELECOM E LA LEGGE ALFANO »	47
	1) La seconda repubblica e il processo SME.....	47
	2) Il processo TELECOM e la Legge 20 novembre 2006 n. 281.....	49
	3) La sentenza 11 giugno 2009 n. 173 della Corte costituzionale.....	51
	4) L'incostituzionalità della Legge Alfano.....	53
8	LA TRATTATIVA STATO – MAFIA E L'AFFAIRE DELLE INTERCETTAZIONI DEL PRESIDENTE DELLA REPUBBLICA GIORGIO NAPOLITANO »	54
	1) La sentenza 15 gennaio 2013 n. 1 della Corte costituzionale.....	54

CAPITOLO SECONDO
NUOVE TECNOLOGIE E INTERCETTAZIONI.
I CAPTATORI INFORMATICI DALLA RIFORMA ORLANDO
A QUELLA BONAFEDE.

1. IL TROJAN HORSE E LA RIFORMA ORLANDO: AFFINAMENTO DELLE TECNICHE	
INVESTIGATIVE E CAPTATORI INFORMATICI.	59
1) La tecnica dell'intrusione diffusa.	59
2) Il "captatore" o "intrusore" informatico e le prime sentenze sulla legittimità del nuovo sistema di raccolta delle prove: la sentenza "Scurato".	61
3) La "Riforma Orlando". Le potenzialità investigative del <i>malware</i> tra diritto di difesa e diritto di cronaca.	63
2 LE CRITICITÀ DELL'IMPIANTO DELLA RIFORMA ORLANDO E L'ITER PARLAMENTARE	
DELLA NUOVA DISCIPLINA DELLE INTERCETTAZIONI.	69
1) Il passaggio parlamentare della Riforma Bonafede.	69
3 IL DIFFICILE APPRODO ALLA RIFORMA BONAFEDE: L'INTRODUZIONE DELLA NUOVA	
DISCIPLINA DELLE INTERCETTAZIONI.	72
1) L'architettura della nuova disciplina delle intercettazioni.	72
2) Il regime transitorio e l'entrata in vigore delle nuove disposizioni.	83

CAPITOLO TERZO
LA RIFORMA BONAFEDE DELLE INTERCETTAZIONI
DI CONVERSAZIONI E COMUNICAZIONI.
(IL PARADIGMA SINCRONICO)

1 LA CORNICE COSTITUZIONALE E L'APPRODO LEGISLATIVO TRA LIBERTÀ	
DI COMUNICAZIONE E DI PENSIERO ED ESIGENZE INVESTIGATIVE.	87
2 LINEE SISTEMATICHE DELLA DISCIPLINA VIGENTE.	93
1) Il sistema normativo.	93
2) Orientamenti giurisprudenziali (Cassazione SS.UU. del 2008).	94
3) Gli assetti organizzativi e gestionali della riforma.	95
3 I CASI E I MODI DELLE INTERCETTAZIONI: LIMITI DI AMMISSIBILITÀ.	
IL CAPTATORE INFORMATICO.	99
1) Il captatore informatico (cd. <i>trojan</i>) e le intercettazioni dei presenti. Limiti e condizioni per il suo utilizzo.	99
2) La riforma Bonafede e le intercettazioni dei parlamentari.	105
4 I CASI E I MODI DELLE INTERCETTAZIONI: PRESUPPOSTI E FORME	
DEL PROVVEDIMENTO.	109
1) Condizioni e modalità.	109

2) Le intercettazioni di urgenza..... »	113
3) I generi trascrittivi..... »	114
5 LE FORME DELLE INTERCETTAZIONI: L'ESECUZIONE DELLE OPERAZIONI.	
LE COSIDDETTE INTERCETTAZIONI PREVENTIVE..... »	116
1) L'operatività esecutive e le cosiddette intercettazioni preventive..... »	116
2) I servizi segreti e le intercettazioni preventive..... »	120
3) Intercettazione e codice della <i>privacy</i> »	121
6 LA CONSERVAZIONE DELLA DOCUMENTAZIONE. L'ARCHIVIO DELLE	
INTERCETTAZIONI..... »	123
1) Premessa sistematico-concettuale..... »	123
2) La normativa di attuazione..... »	124
3) L'archivio digitale..... »	125
4) Riforma Bonafede e CAD..... »	131
7 L'UTILIZZAZIONE DELLE INTERCETTAZIONI E I DIVIETI DI UTILIZZAZIONE..... »	133
1) Profili introduttivi..... »	133
2) Le disposizioni del d.lgs. Orlando..... »	135
3) L'art. 270-bis c.p.p..... »	137
8 COMUNICAZIONI DI SERVIZIO DI APPARTENENTI AL DIPARTIMENTO DELLE	
INFORMAZIONI PER LA SICUREZZA E AI SERVIZI DI INFORMAZIONE	
PER LA SICUREZZA..... »	138
1) L'AISE e L'AISI nel sistema delle intercettazioni..... »	138
2) Il segreto nella legge n. 124 del 2007..... »	140
9 LE ALTRE PRINCIPALI DISPOSIZIONI NOVELLATE DALLA RIFORMA..... »	143
1) Generalità..... »	143
2) Le misure di cautela..... »	143
3) L'avviso di conclusione indagini..... »	146
4) La trascrizione..... »	148
10 PROFILI DI RESPONSABILITÀ, IL DIVIETO DI PUBBLICAZIONE E LA SUA VIOLAZIONE.	
BREVI CENNI E CONCLUSIONI..... »	149
• BIBLIOGRAFIA E SITOGRAFIA..... »	163
• APPENDICE PARTE PRIMA.	
I pareri tecnici alla riforma Bonafede. (Una diacronia prospettica)..... »	167
• APPENDICE PARTE SECONDA.	
Rassegna giurisprudenziale. (Una sincronia prospettica)..... »	199
• APPENDICE PARTE TERZA.	
La legislazione vigente..... »	215

1

**IL TROJAN HORSE E LA RIFORMA ORLANDO: AFFINAMENTO DELLE
TECNICHE INVESTIGATIVE E CAPTATORI INFORMATICI.****1) LA TECNICA DELL'INTRUSIONE DIFFUSA.**

L'affinamento delle tecniche investigative legate sempre più allo sviluppo delle tecnologie informatiche, proiettarono gli strumenti di raccolta della prova ben oltre le colonne d'Ercole dell'immaginabile. Parafrasando i versi danteschi che delineavano i tratti del *più noto dei furbi* ma al tempo stesso del primo dannato dalla fame di “*virtute e canoscenza*”, i pirati informatici (*hacker*), intuito il potenziale economico che sarebbe derivato del nascente mercato dei dati personali, idearono, chiamandolo con il nome del più famoso inganno della storia dell'umanità, un sistema di intrusione nei dispositivi elettronici dei malcapitati al fine di controllarli e trarne informazioni sensibili⁽⁹⁰⁾.

⁽⁹⁰⁾ “*A rendere prioritaria tale minaccia contribuiscono altresì le sfide poste dagli aspetti peculiari che la caratterizzano. Essa, infatti, si presenta come pervasiva, sofisticata, eseguibile con strumenti di facile accesso ed uso, rapida nelle evoluzioni e dotata di elevata capacità di rimodulazione rispetto agli strumenti posti di volta in volta a difesa di reti e sistemi. A complicare ulteriormente tale contesto, interviene inoltre la circostanza che gran parte delle attività intrusive si configurano come anonime, ingannevoli e condotte da soggetti sovente di difficile identificazione grazie all'impiego di dispositivi che permettono l'uso delle identità digitali degli internauti e dei dispositivi connessi alle reti appartenenti a terzi inconsapevoli [...] Quanto al modus operandi, tali attività hanno consentito di rilevare il prevalente ricorso a malware già noti e sovente reingegnerizzati. All'elevato livello di organizzazione e sofisticazione raggiunto dagli attaccanti, anche in ragione della loro crescente capacità di combinare sinergicamente diverse tipologie di vettori di penetrazione, ha fatto da contrappeso, da parte dei soggetti target, la scarsa percezione della minaccia e della necessità di adeguate contromisure. La ricerca info-operativa non ha mancato di registrare episodi di sottrazione informativa, specie di natura finanziaria, da parte della criminalità organizzata. Significative, in tale ambito, le acquisizioni attestanti il rapido accrescimento di vettori di attacco verso piattaforme mobili, segnatamente quelle di mobile banking; la diffusione di siti web dannosi o infetti per la distribuzione di malware; il lancio in elevati volumi di campagne di spam, finalizzate a promuovere false offerte commerciali; l'inoculazione nei sistemi degli utenti di codici maligni (emblematici quelli occultati all'interno di file allegati ad e-mail ed indirizzati a target remunerativi, il cd. spear phishing); il massiccio impiego di ransomware ovvero del blocco di un sistema a scopo di riscatto. Particolarmente indicativi sono apparsi, poi, i segnali del coinvolgimento di realtà criminali in attività di spionaggio industriale - finalizzate alla sottrazione di brevetti industriali, piani aziendali, studi e ricerche di mercato, analisi e descrizioni dei processi produttivi, etc. – attività di cui non si esclude una committenza da parte di competitor”, Relazione sulla politica dell'informazione per la sicurezza, 2013.*

Per *trojan horse* (letteralmente, *cavallo di Troia*) viene comunemente inteso un programma, apparentemente utile, che contiene funzioni nascoste atte ad abusare dei privilegi dell'utente (proprietario/utilizzatore del dispositivo elettronico) che lo esegue fornendo all'*hacker*, una comoda porta d'accesso, *backdoor*, grazie alla quale potrà reintrodursi successivamente nel sistema autonomamente.

Da un punto squisitamente tecnico il *trojan* è un programma compilato o in un linguaggio di programmazione ad alto livello come il linguaggio C, C++, Java oppure un semplice *JavaScript* in una pagina *web*, che utilizza, nella maggior parte dei casi un semplice e collaudato paradigma di interdipendenza *client/server*, laddove il *client* viene installato sul dispositivo dell'*hacker* mentre il *server* è posto sul dispositivo del soggetto da controllare. Il meccanismo di funzionamento è molto semplice, quasi banale: il *server*, una volta attivato, si mette *in ascolto* su di una o più porte di comunicazione del dispositivo (porte TCP) e attende che il *client* dell'*hacker* si connetta ad una di quelle porte in modo da poter stabilire un collegamento tra i due dispositivi.

Avvenuta la connessione, l'*hacker* è libero di poter controllare da remoto l'altro dispositivo con la possibilità, fungendo anche da *keylogger*, di registrare gli *input* digitati da tastiera acquisendo in tempo reale le *chat* delle piattaforme social nonché delle più comuni applicazioni di messaggistica istantanea protette da crittografia del tipo “*end to end*”⁽⁹¹⁾, potendo, tra l'altro, anche geolocalizzare il dispositivo, scattare foto, attivare la videocamera o il microfono. I *trojan* più comuni e diffusi hanno le sembianze di una *utility*, di uno *screensaver*, di un *videogame* facilmente reperibili sul *web* o possono essere introdotti nella macchina attraverso l'allegato di una *mail*; una volta mandati in esecuzione, installano, all'insaputa del proprietario, il file *server*, che si maschera all'interno del sistema.

⁽⁹¹⁾ Il sistema di funzionamento della crittografia *end to end*, in uso su quasi tutte le piattaforme social e di messaggistica istantanea è molto semplice. Quando l'utente aggiunge un contatto alla propria rubrica, l'applicazione di messaggistica (*WhatsApp* ad esempio) presente sul cellulare dell'utente si connette creando, in sincrono con quella del contatto aggiunto, due coppie di chiavi interdipendenti. Le chiavi di cifratura, segrete, vengono archiviate sui rispettivi dispositivi e sono invisibili anche alla applicazione di messaggistica stessa; di fatti quando l'utente andrà ad inviare un messaggio con *WhatsApp*, il *server* dell'azienda lo riceverà e lo indirizzerà al destinatario, ma non sarà in grado di decifrarlo e leggerlo. Ampiamente sul tema O. CALAVITA, *La contro-riforma Bonafede delle intercettazioni: sul captatore informatico rimangono alcune perplessità*, su *Istituzioni Diritto Economia (Online)*, Vol. 2, N. 1, 2020, p. 155 e seg.; M. TORRE, *Il captatore informatico. Nuove Tecnologie investigative e rispetto delle regole processuali*, Giuffrè. 2017, pp. 13 e ss.

2) IL “CAPTATORE” O “INTRUSORE” INFORMATICO E LE PRIME SENTENZE SULLA LEGITTIMITÀ DEL NUOVO SISTEMA DI RACCOLTA DELLE PROVE: LA SENTENZA “SCURATO”.

Le potenzialità di tale innovativo sistema venivano, di converso, colte dagli investigatori i quali trasformarono tale tecnica di intrusione in un vero e proprio mezzo di ricerca della prova, detto appunto, a mezzo del “*captatore*” o “*intrusore*” informatico rivoluzionando, così, il sistema delle intercettazioni. Già a partire dal 2011 tale sistema iniziò ad essere utilizzato dalle Procure consentendo di trasformare, di fatto, i dispositivi elettronici dei soggetti sottoposti ad indagini in vere e proprie “*cimici*”⁽⁹²⁾. La prima indagine ad essere condotta utilizzando il sistema del *trojan*, mascherato nel dispositivo dell’indagato con il nome “*Querela*”, fu l’inchiesta della Procura della Repubblica di Napoli sulla loggia massonica *P4* e sul faccendiere Luigi Bisignani. Ovviamente i nuovi metodi di captazione dovevano necessariamente integrarsi ed armonizzarsi con l’intero sistema del processo penale cosa che sulle prime non avvenne. Difatti la Cassazione, VI Penale, con la sentenza n. 27100 del 26 giugno 2015⁽⁹³⁾, dichiarò l’inutilizzabilità di tale sistema di intercettazioni, anche nei processi relativi alla criminalità organizzata, in quanto, il decreto autorizzativo del G.i.p. non era in grado di individuare il luogo per il quale l’intercettazione veniva autorizzata. La Suprema Corte osservò come l’attivazione a distanza del microfono o della videocamera del dispositivo controllato con il *trojan* configurasse una ipotesi di intercettazione ambientale senza limitazione spaziale alcuna in quanto l’operatore avrebbe potuto vedere e ascoltare l’intercettato in qualsiasi posto esso si fosse recato portando con sé il dispositivo. Tanto apparve in evidente contrasto con il precetto costituziona-

⁽⁹²⁾ Il termine gergale “*cimice*” è comunemente usato per intendere una microspia. Grazie alle sue ridotte dimensioni può facilmente essere celata sia in ambiente domestico che lavorativo, potendosi nascondere e mascherare in qualsiasi oggetto (ad esempio all’interno di batterie di telefoni cellulari, prese, penne, lampade da ufficio, fogli di carta, ciondoli e portachiavi ecc.) e anche nei capi di abbigliamento. Il principio base di funzionamento di una cimice microspia è quello di generare delle onde radio da trasmettere nell’etere. Il microfono della cimice capta l’audio, le voci, le conversazioni e anche i rumori che si svolgono nell’ambiente in cui è localizzata la spia stessa mentre il trasmettitore genera le onde radio che, una volta trasmesse, saranno captate da un ricevitore a distanza.

⁽⁹³⁾ “*L’intercettazione di conversazioni tramite il c.d. agente intrusore, che consente la captazione “da remoto” delle conversazioni tra presenti mediante l’attivazione, attraverso il c.d. virus informatico, del microfono di un apparecchio telefonico smartphone, dà luogo ad un’intercettazione ambientale che può ritenersi legittima, ai sensi dell’art. 266, comma secondo, cod. proc. pen. in relazione all’art. 15 Cost., solo quando il decreto autorizzativo individui con precisione i luoghi in cui espletare l’attività captativa*”, Cass. Pen., Sez. VI, ordinanza 26 giugno 2015 n. 13884, CED Cassazione, 2015.

le di cui all'art. 15 Cost. nonché con l'art. 266 secondo comma c.p.p., avendo il legislatore previsto che l'intercettazione potesse svolgersi solo nel luogo individuato dal decreto autorizzativo del G.i.p.

Nel 2016 la VI Sez. Penale della Corte di cassazione, con l'ordinanza 10 marzo 2016 n. 13884, tornò sull'argomento affermando come la predeterminazione dei luoghi in cui attivare il captatore dovesse avvenire solo ed esclusivamente nei casi in cui la captazione si stesse svolgendo nei luoghi di cui all'art. 614 c.p.

Tuttavia, la Cassazione, prevenendo l'insorgere di contrasti giurisprudenziali, rimise alla Sezioni Unite la questione se *“anche nei luoghi di privata dimora, pure non singolarmente individuati ed anche se ivi non si stia svolgendo l'attività criminosa, sia consentita l'intercettazione di conversazioni o comunicazioni tra presenti, mediante personal computer, tablet, smartphone”*.

La Cassazione Penale a Sezioni Unite, con la sentenza 26 aprile 2016 n. 26889, chiarì definitivamente come l'utilizzo del moderno strumento del *trojan* non consentisse a priori l'individuazione dei luoghi in cui l'ascolto, a mezzo del dispositivo controllato, potesse avvenire né, tanto meno, se in quei luoghi si stesse svolgendo una quale attività illecita statuendo come in tema di intercettazioni *“itineranti”*⁽⁹⁴⁾, mediante utilizzo di *trojan* (*captatore o intrusore informatico*), nel caso di reati di criminalità organizzata si potesse ben prescindere dal riferimento ad un determinato luogo, in quanto, nei limiti in cui si disponesse sul piano tecnico di strumenti idonei ad assicurare la captazione delle conversazioni, fosse comunque legittimo il ricorso ad operazioni di intercettazione anche in luoghi di privata dimora.

La Cassazione esclude, quindi, l'utilizzabilità di tale metodica in tutti gli altri casi che non riguardassero la criminalità organizzata, in quanto non avrebbe consentito di determinare preventivamente il luogo della captazione, a fronte

⁽⁹⁴⁾ *“In realtà, a ben vedere, proprio sulla base della considerazione svolta dalle Sezioni Unite, secondo cui il giudice non può previamente conoscere il domicilio intercettato, non può negarsi che l'intercettazione “itinerante”, al pari delle riprese visive, non sia previsto dalla legge, né sia sottoposto al controllo giurisdizionale quanto ai domicili che potranno essere violati, sottraendosi così alla “riserva” sia di legge, sia di giurisdizione, ex artt. 14 e 15 Cost. e perciò esso è pacificamente inammissibile. Ciò è confermato anche dalle iniziative parlamentari tese all'approvazione di modifiche legislative che prevedano specificamente l'impiego della nuova tecnologia investigativa. Tutto il sistema normativo, costituzionale, sovranazionale e codicistico, in materia di intercettazioni è teso a consentire limitazioni della segretezza delle comunicazioni e del domicilio nel rispetto dei principi della riserva di legge e di giurisdizione, di “stretta necessità”, della “proporzionalità” tra esigenze di repressione penale e sicurezza pubblica e di tutela delle libertà del singolo e della “prevedibilità” delle ingerenze pubbliche nei diritti del cittadino”, L. FILIPPI, L'intercettazione “itinerante” una prova incostituzionale, in *Quotidiano Giuridico*, Wolters Kluwer Italia, 2016.*

del limite dettato dall'art. 266, comma 2, c.p.p., secondo il quale le intercettazioni ambientali possono essere effettuate in luogo di privata dimora solo se ivi sia in corso una qualche attività criminosa.

La necessità di una disciplina specifica dell'utilizzo del *trojan* emerse con forza dalla sentenza "Scurato" delle Sezioni Unite a seguito della quale si rese necessario e non più procrastinabile l'intervento del legislatore al fine, non solo, di recepire gli intervenuti orientamenti giurisprudenziali ma anche di superare le continue critiche relative alla scarsa attitudine garantista della disciplina.

Come vedremo d'appresso, la risposta del legislatore non si fece attendere.

3) LA "RIFORMA ORLANDO". LE POTENZIALITÀ INVESTIGATIVE DEL *MALWARE* TRA DIRITTO DI DIFESA E DIRITTO DI CRONACA.

Il 29 dicembre 2017, a quasi un anno dello scoppio del caso CONSIP⁽⁹⁵⁾, venne approvato il decreto legislativo n. 216, più comunemente conosciuto come "Riforma Orlando", dal Guardasigilli proponente, in attuazione della delega al Governo contenuta nell'art. 1, commi 82⁽⁹⁶⁾, 83⁽⁹⁷⁾ e 84 lett. a) e b) c) d) ed e)

⁽⁹⁵⁾ Verso la fine del dicembre 2016, le agenzie di stampa italiane riportarono la notizia di una inchiesta, avviata dai P.M. napoletani Henry John Woodcock e Celeste Carano, relativa a un presunto caso di corruzione di un dirigente della CONSIP (Concessionaria Servizi Informativi Pubblici) da parte dell'imprenditore campano Alfredo Romeo. L'inchiesta coinvolgeva anche Luca Lotti, ministro dello sport del Governo Renzi e Tullio Del Sette, Comandante Generale dei Carabinieri in quanto, secondo l'accusa, avrebbero rivelato l'esistenza dell'indagine all'amministratore delegato di Consip, Luigi Marroni e al presidente Luigi Ferrara.

⁽⁹⁶⁾ "Il Governo è delegato ad adottare decreti legislativi per la riforma della disciplina in materia di intercettazione di conversazioni o comunicazioni e di giudizi di impugnazione nel processo penale nonché per la riforma dell'ordinamento penitenziario, secondo i principi e criteri direttivi previsti dai commi 84 e 85", art. 1 comma 82, L. 23 giugno 2017 n. 103.

⁽⁹⁷⁾ "I decreti legislativi di cui al comma 82 sono adottati, su proposta del Ministro della giustizia, relativamente alle materie a cui si riferiscono i principi e criteri direttivi di cui alle lettere a), b), c), d) ed e) del comma 84 nel termine di tre mesi, e relativamente alle restanti materie nel termine di un anno, senza nuovi o maggiori oneri per la finanza pubblica. I termini per l'esercizio delle deleghe decorrono dalla data di entrata in vigore della presente legge. I relativi schemi sono trasmessi alle Camere, corredati di relazione tecnica che dia conto della neutralità finanziaria dei medesimi, per l'espressione dei pareri delle Commissioni parlamentari competenti per materia e per i profili finanziari. I pareri sono resi nel termine di quarantacinque giorni, decorsi i quali i decreti possono essere comunque emanati. Qualora tale termine venga a scadere nei trenta giorni antecedenti la scadenza del termine di delega, o successivamente, quest'ultimo termine è prorogato

3) GLI ASSETTI ORGANIZZATIVI E GESTIONALI DELLA RIFORMA.

L'attuazione della disciplina ha comportato uno sforzo organizzativo, formativo e di investimento infrastrutturale notevole. Il dipartimento dell'organizzazione giudiziaria, del personale e dei servizi offre un servizio di assistenza tecnica per l'avvio a tutte le 140 procure della Repubblica, nonché il servizio di *help desk* organizzativo destinato alla segnalazione delle esigenze di carattere organizzativo e logistico a cui, proprio dal 1° settembre, si è affiancato il servizio di assistenza per la configurazione delle postazioni dell'archivio digitale. Le indicazioni e le circolari diramate al riguardo dal dipartimento dell'organizzazione giudiziaria, del personale e dei servizi, al fine di accompagnare l'avvio dell'operatività dei nuovi sistemi di intercettazione sviluppa in una serie di testi normativi e regolamentari di cui, qui di seguito, si offre un completo compendio. Il 31 agosto 2020 il dipartimento completa l'azione di digitalizzazione e securizzazione delle intercettazioni. In precedenza, l'attività svolta segnava le seguenti tappe.

Il 18 luglio del 2013 il garante per la protezione dei dati personali adottava il relativo provvedimento in materia di misure di sicurezza nelle attività di intercettazione da parte delle procure della Repubblica. In occasione della presentazione del disegno di legge AS1659, di conversione in legge del decreto nr. 161 del 2019 *cit.*, il presidente dell'*Authority* veniva udito presso il Senato della Repubblica. Dal 4 febbraio 2020 non si segnalano ulteriori atti del garante per la protezione dei dati personali.

Con le circolari del 4 e del 14 maggio del 2018 il dipartimento ministeriale offre indicazioni operative ai fini dell'attuazione dell'art. 269 c.p.p. e dell'art. 89-*bis* disp. att. c.p.p. laddove, con d.m. 20 aprile 2018 venivano recate le disposizioni di attuazione per le intercettazioni mediante inserimento di captatore informatico e per l'accesso all'archivio informatico a norma dell'art. 7, commi 1 e 3, del decreto legislativo 29 dicembre 2017, nr. 216.

Nell'ambito delle indicazioni operative inerenti al completamento della digitalizzazione e securizzazione delle intercettazioni e delle ulteriori conseguenti attività logistico-organizzative ex artt. 269 c.p.p. e 89-*bis* disp. att. c.p.p. si devono segnalare le circolari del 2 dicembre 2019 di richiamo della circolare del 4 aprile 2018 sfociate nel provvedimento del direttore generale dei servizi informativi automatizzati di adozione delle specifiche tecniche per il conferimento nell'archivio riservato delle intercettazioni di cui all'art. 269 co.1 c.p.p. A tanto il direttore della DGSIA ha provveduto in data 5 dicembre 2019.

Il 31 gennaio 2020, a seguito dell'incontro del 21 gennaio 2020, vengono offerte le indicazioni operative ai fini dell'art. 269 c.p.p. e 89-*bis* disp. att. c.p.p. così come modificati dal decreto-legge 30 dicembre 2019 nr.161. Ulteriori

indicazioni operative in tema di intercettazioni e relative attività formative vengono in seguito offerte dalla circolare 24 aprile 2020.

Il 6 maggio del medesimo anno il ministero si occupa della gestione delle intercettazioni e dell'archivio riservato con seminari informativi rivolti alle procure della Repubblica e ai tribunali – area penale – nonché tribunali e procure della Repubblica settore minorile. Ventuno giorni dopo, il 27 maggio 2020, si ha il completamento della digitalizzazione e securizzazione delle intercettazioni e delle ulteriori conseguenti attività logistico e organizzativo ex artt. 269 c.p.p. e 89-*bis* disp. att. c.p.p. per il tramite di indicazioni specifiche.

In data 14 luglio 2020 viene emanata una circolare sulla gestione delle intercettazioni. Precisamente rivolta alle procure della Repubblica e all'area penale dei tribunali sull'applicativo archivio documento. Medesima circolare tre giorni dopo, il 17 di luglio, viene emanata per il settore minorile.

Il 20 luglio del 2020 vengono offerte le ultime indicazioni operative sul completamento della digitalizzazione e securizzazione delle intercettazioni e delle ulteriori conseguenti attività logistico e organizzative ex art. 269 c.p.p. e 89-*bis* disp. att. c.p.p.

In seguito, si approda alla circolare di completamento già citata in avvio di discorso del 31 agosto 2020. Il giorno dopo, la novella legislativa in tema di intercettazioni è in vigore sull'intero territorio nazionale.

L'attività logistico organizzativa del Ministero della Giustizia non si ferma qui. Per il tramite di un accesso sezionele dedicato è consentito al personale, individuato e comunicato dagli uffici interessati, di consultare i *link* funzionali in termini di attività pratica quali ad esempio il portale dei servizi telematici giustizia dove è pubblicato il materiale informativo ed operativo realizzato dalla DGSIA e destinato agli avvocati.

Va da ultimo segnalata la piattaforma *e-learning* per la formazione a distanza dell'organizzazione giudiziaria in cui uno spazio è dedicato al tema delle intercettazioni e contiene il più rilevante materiale sinora prodotto dal dipartimento dell'organizzazione giudiziaria ministeriale, nonché una raccolta di documentazione normativa e regolamentare in materia di intercettazioni. Per gli accessi alla sezione e per le necessarie informazioni gli uffici giudiziari possono contattare il cd. Ufficio II di formazione della direzione generale del personale e della formazione ad una *mail* dedicata.

Sotto il terzo versante, quello della normativa primaria, paradigma normativo, come vedremo, resta l'art. 266 c.p.p. così come novellato dalla riforma.

La novella ha inciso in modo determinante sulle norme di attuazione, di coordinamento e transitorie del Codice di procedura penale con l'inserimento dell'art. 89-*bis* istituendo l'archivio riservato delle intercettazioni. A tal proposito va segnalato il modello di protocollo d'intesa tra la procura della Repubblica e la procura per i minorenni riguardante l'esercizio del diritto di ac-

cesso all'archivio delle intercettazioni da parte dei soggetti indicati dall'art. 89-bis, co. 3 delle norme di attuazione, di coordinamento e transitorie del Codice di procedura penale.

Nel medesimo segno di compendio normativo di riferimento la normativa primaria si sostanzia nelle seguenti leggi della Repubblica che all'attualità regolano il sistema delle intercettazioni in Italia. Innanzitutto, il decreto-legge nr. 28 del 30 aprile 2020 recante le misure urgenti per la funzionalità dei sistemi di intercettazione di conversazioni e comunicazioni, ulteriori misure urgenti in materia di ordinamento penitenziario, nonché disposizioni integrative e di coordinamento in materia di giustizia civile, amministrativo e contabile, e misure urgenti per l'introduzione del sistema di allerta covid-19.

Vanno quindi segnalati i decreti-legge 30 dicembre 2019, nr. 161 e 29 dicembre 2009 nr. 193, rispettivamente dedicati alle modifiche urgenti alla disciplina delle intercettazioni e agli interventi urgenti in materia di funzionalità del sistema giudiziario.

In materia rileva altresì il d.m. 20 aprile 2018, recante disposizioni di attuazione per le intercettazioni mediante inserimento di captatore informatico e per l'accesso all'archivio informatico a norma dell'art. 7 commi 1 e 3, del decreto legislativo 29 dicembre 2017, nr. 216. Quest'ultimo provvedimento normativo è proprio quello recante le prime disposizioni in materia di intercettazioni di conversazioni o comunicazioni in attuazione della delega di cui all'art.1, commi 82, 83 e 84, lett. a), b), c), d) ed e) della legge – cd. Orlando – del 23 giugno 2017, nr. 103, recante modifiche al Codice penale, al Codice di procedura penale e all'ordinamento penitenziario.

Il quadro normativo di riferimento tracciato si completa col regolamento concernente le regole tecniche per l'adozione nel processo civile e nel processo penale, delle tecnologie delle informazioni e della comunicazione.

L'articolata piattaforma normativa di cui abbiamo offerto conto compiutamente nelle pagine che precedono costituisce l'imprescindibile base per poter comprendere la vastità e la complessità del nuovo sistema di captazione giudiziaria elaborato dal nostro sistema giuridico. L'indicata piattaforma normativa offre il corpo tecnico per poter operare con il novellato strumentario degli artt. 266 e seg. c.p.p. nel quadro dei valori sottesi alla riforma. Si è detto che la novella sulle intercettazioni entrata in vigore il 1° settembre del 2020 è il frutto, tra l'altro, di una sovrapposizione normativa tra la riforma Orlando e gli emendamenti Bonafede. Orbene nelle pagine successive daremo conto dello stato dell'arte della normativa all'attualità – la vigente disciplina in materia di intercettazioni nel nostro Paese – non tralasciando brevi, brevissimi spunti di ragguaglio comparativo tra i provvedimenti Orlando e quello Bonafede al fine di consentire al lettore una massima intellegibilità del sistema, anche sotto il versante della *ratio* che ha guidato il

legislatore nell'approdare all'indicata riforma⁽¹⁴⁷⁾.

I punti che seguono rassegnano nel dettaglio la disciplina delle intercettazioni di cui si tratta; non solo, verranno offerte, altresì, compiute indicazioni sull'insieme della novella anche allorquando essa non incide direttamente sul corpo normativo degli artt. 266 e seg. c.p.p. e delle relative norme di attuazione come, ad esempio, in tema di pubblicazione di atti o di registrazione delle pertinenti operazioni captative.

⁽¹⁴⁷⁾ I temi trattati nel testo, a testimoniare la fondamentale importanza per la comprensione del sistema, sono stati oggetto di uno dei primi scritti intervenuti all'esito dell'entrata in vigore della novella. Ci si riferisce al già citato S. RICCHITELLI, *Prolegomeni allo studio della riforma delle intercettazioni di conversazioni o comunicazioni*, ove si è offerto compiuto conto delle ragioni per le quali senza la comprensione del tritico giurisprudenza previgente – normativa secondaria – normativa primaria non si può avere un compiuto quadro concettuale del sistema inerente al mezzo di ricerca probatorio in disamina funzionale alle esigenze degli addetti ai lavori e di coloro che vogliono avere complete e compiute informazioni circa la disciplina delle intercettazioni di conversazioni o comunicazioni oggi vigente nel nostro Paese.

8

**COMUNICAZIONI DI SERVIZIO DI APPARTENENTI
AL DIPARTIMENTO DELLE INFORMAZIONI PER LA SICUREZZA
E AI SERVIZI DI INFORMAZIONE PER LA SICUREZZA.**

1) L'AISE E L'AISI NEL SISTEMA DELLE INTERCETTAZIONI.

Un'altra novità della riforma Orlando-Bonafede in materia di intercettazioni è sicuramente costituita dall'inserimento di una fattispecie procedimentale ad *hoc* nel quadro della disciplina della ricerca probatoria per il tramite di intercettazioni. Si tratta della norma che contempla le comunicazioni di servizio di appartenenti al DIS (Dipartimento delle Informazioni per la Sicurezza) e all'AISE ed all'AISI (Servizi di Informazione per la Sicurezza).

È noto che il sistema procedimentale italiano, a differenza di altri Paesi (ad esempio la Svizzera) non implica rapporti diretti tra autorità giudiziaria, in particolare inquirente, ed esponenti dei servizi segreti. Tale contesto normativo è stratificato da decenni nel nostro sistema processuale ed il Codice di procedura del '89 lo ha rinvenuto intonso dalla normativa di riferimento precedente.

Bisogna a tale scopo tener presente che la normativa sui servizi segreti, in origine SISDE e SISMI poi divenuti AISE e AISI, è stata completamente rivoluzionata nel 2007 ad opera della legge nr. 124 del 3 agosto di quello stesso anno. Sino a quel momento, ma con una vigenza che permane fino ai giorni nostri, l'unico luogo del Codice di procedura penale nel quale si faceva riferimento ai servizi di sicurezza era la norma scritta in materia di testimonianza quale mezzo di prova all'art. 203 c.p.p. In particolare, questa norma, dedicata agli informatori della P.G. e dei Servizi, aveva la sola funzione di stabilire che il giudice non può obbligare gli ufficiali e gli agenti di polizia giudiziaria nonché il personale dipendente dai Servizi per le informazioni per la sicurezza militare o democratica a rivelare i modi dei loro informatori. Se questi non sono esaminati come testimoni le informazioni da essi fornite non possono essere acquisite né utilizzate. L'inutilizzabilità opera anche nelle fasi diverse dal dibattimento, se gli informatori non sono stati interrogati né assunti a sommarie informazioni.

Tale disposizione processuale, inserita nel contesto normativo delle norme dedicate al segreto professionale d'ufficio e di Stato trovava una parziale temperanza nella disposizione in virtù della quale non possono essere oggetto di segreto d'ufficio, di segreto di Stato o di informazione non rilevabile i fatti, le notizie o i documenti concernenti reati diretti all'eversione dell'ordinamento costituzionale nonché i delitti previsti dagli artt. 285, 416-*bis*, 416-*ter* e 422

del Codice penale⁽²¹⁰⁾.

⁽²¹⁰⁾ “1. Con il provvedimento che dispone la custodia cautelare, il giudice ordina agli ufficiali e agli agenti di polizia giudiziaria che l'imputato sia catturato e immediatamente condotto in un istituto di custodia per rimanervi a disposizione dell'autorità giudiziaria. 2. Prima del trasferimento nell'istituto la persona sottoposta a custodia cautelare non può subire limitazione della libertà, se non per il tempo e con le modalità strettamente necessarie alla sua traduzione. 3. Per determinare la pena da eseguire, la custodia cautelare subita si computa a norma dell'articolo 657, anche quando si tratti di custodia cautelare subita all'estero in conseguenza di una domanda di estradizione ovvero nel caso di rinnovamento del giudizio a norma dell'articolo 11 del Codice penale”, art. 285 c.p.p.; “Chiunque fa parte di un'associazione di tipo mafioso formata da tre o più persone, è punito con la reclusione da dieci a quindici anni. Coloro che promuovono, dirigono o organizzano l'associazione sono puniti, per ciò solo, con la reclusione da dodici a diciotto anni. L'associazione è di tipo mafioso quando coloro che ne fanno parte si avvalgono della forza di intimidazione del vincolo associativo e della condizione di assoggettamento e di omertà che ne deriva per commettere delitti, per acquisire in modo diretto o indiretto la gestione o comunque il controllo di attività economiche, di concessioni, di autorizzazioni, appalti e servizi pubblici o per realizzare profitti o vantaggi ingiusti per sé o per altri, ovvero al fine di impedire od ostacolare il libero esercizio del voto o di procurare voti a sé o ad altri in occasione di consultazioni elettorali. Se l'associazione è armata si applica la pena della reclusione da dodici a venti anni nei casi previsti dal primo comma e da quindici a ventisei anni nei casi previsti dal secondo comma. L'associazione si considera armata quando i partecipanti hanno la disponibilità, per il conseguimento della finalità dell'associazione, di armi o materie esplosive, anche se occultate o tenute in luogo di deposito. Se le attività economiche di cui gli associati intendono assumere o mantenere il controllo sono finanziate in tutto o in parte con il prezzo, il prodotto, o il profitto di delitti, le pene stabilite nei commi precedenti sono aumentate da un terzo alla metà. Nei confronti del condannato è sempre obbligatoria la confisca delle cose che servirono o furono destinate a commettere il reato e delle cose che ne sono il prezzo, il prodotto, il profitto o che ne costituiscono l'impiego. Le disposizioni del presente articolo si applicano anche alla camorra, alla 'ndrangheta e alle altre associazioni, comunque localmente denominate, anche straniere, che valendosi della forza intimidatrice del vincolo associativo perseguono scopi corrispondenti a quelli delle associazioni di tipo mafioso”, art. 416-bis c.p.p.; “Chiunque accetta, direttamente o a mezzo di intermediari, la promessa di procurare voti da parte di soggetti appartenenti alle associazioni di cui all'articolo 416-bis o mediante le modalità di cui al terzo comma dell'articolo 416-bis in cambio dell'erogazione o della promessa di erogazione di denaro o di qualunque altra utilità o in cambio della disponibilità a soddisfare gli interessi o le esigenze dell'associazione mafiosa è punito con la pena stabilita nel primo comma dell'articolo 416-bis. La stessa pena si applica a chi promette, direttamente o a mezzo di intermediari, di procurare voti nei casi di cui al primo comma. Se colui che ha accettato la promessa di voti, a seguito dell'accordo di cui al primo comma, è risultato eletto nella relativa consultazione elettorale, si applica la pena prevista dal primo comma dell'articolo 416-bis aumentata della metà. In caso di condanna per i reati di cui al presente articolo, consegue sempre l'interdizione perpetua dai pubblici uffici”, art. 416-ter c.p.p.; “1. Quando non provvede a norma del comma 4 dell'articolo 421, ovvero a norma dell'articolo 421-bis, il giudice può disporre, anche d'ufficio, l'assunzione delle prove

Se viene opposto il segreto, la natura del reato è definita dal giudice. Prima dell'esercizio dell'azione penale provvede il G.I.P. su richiesta di parte.

Non possono altresì essere oggetto del segreto fatti, notizie o documenti concernenti le condotte attuate da appartenenti ai servizi di informazione per la sicurezza in violazione della disciplina concernente la speciale causa di giustificazione prevista per attività del personale dei servizi informazione per la sicurezza.

Si considerano violazioni della già menzionata disciplina le condotte per le quali essendo stata esperita l'apposita procedura prevista dalla legge risulta esclusa l'esistenza della speciale causa di giustificazione.

2. IL SEGRETO NELLA LEGGE N. 124 DEL 2007.

La disciplina del segreto così come ora compendiate è stata completamente innovata dalla citata legge nr. 124 del 2007 *cit.*⁽²¹¹⁾. La citata legge completa le disposizioni su rappresentate statuendo che il segreto di Stato non può essere opposto o confermato ad esclusiva tutela della classifica di segretezza o in ragione esclusiva della natura del documento dell'atto o della cosa oggetto della classifica. In nessun caso il segreto di Stato è opponibile alla Corte costituzionale la quale adotta le necessarie garanzie per la segretezza del procedimento. Quando il Presidente del Consiglio dei ministri non ritenga di confermare il segreto di stato provvede in qualità di autorità nazionale per la sicurezza a declassificare gli atti, i documenti, le copie o i luoghi oggetto di classifica di segretezza, prima che siano messi a disposizione dell'autorità giudiziaria competente. Del provvedimento che rigetta l'eccezione di segretezza è data comunicazione al Presidente del Consiglio dei ministri. Come agevolmente evincibile da quanto si è venuto dicendo sin qui le interrogazioni tra servizi ed

delle quali appare evidente la decisività ai fini della sentenza di non luogo a procedere. 2. Il giudice, se non è possibile procedere immediatamente all'assunzione delle prove, fissa la data della nuova udienza e dispone la citazione dei testimoni, dei periti, dei consulenti tecnici e delle persone indicate nell'articolo 210 di cui siano stati ammessi l'audizione o l'interrogatorio. 3. L'audizione e l'interrogatorio delle persone indicate nel comma 2 sono condotti dal giudice. Il pubblico ministero e i difensori possono porre domande, a mezzo del giudice, nell'ordine previsto dall'articolo 421, comma 2. Successivamente, il pubblico ministero e i difensori formulano e illustrano le rispettive conclusioni. 4. In ogni caso l'imputato può chiedere di essere sottoposto all'interrogatorio, per il quale si applicano le disposizioni degli articoli 64 e 65. Su richiesta di parte, il giudice dispone che l'interrogatorio sia reso nelle forme previste dagli articoli 498 e 499", art. 422 c.p.p.;
⁽²¹¹⁾ Legge 3 agosto 2007, nr. 124 in Gazzetta Ufficiale nr. 187 del 13 agosto 2007 recante il sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto.

autorità giudiziaria non sono in radice recidibili giacché lo stesso Codice di procedura penale in taluni casi quali quelli appena indicati le dà per implicate. D'altro canto, basta scorrere il sistema della citata legge nr. 124 del 2007 per comprendere che gli esponenti di servizi segreti lungi dall'essere *legibus soluti* sono soggetti ad una disciplina particolarmente penetrante sotto il versante delle disposizioni organizzative⁽²¹²⁾.

A fronte di tale compendio normativo non si poteva eludere la circostanza, pur capitata nell'applicazione pratica, di captazioni ex artt. 266 e seg. c.p.p. di appartenenti ai servizi segreti. Tale problematica è stata oggetto di ampio dibattito ministeriale prima e parlamentare poi, giacché il legislatore non è voluto intervenire sul tessuto normativo della legge n. 124 *cit.* ma ha voluto disciplinare, all'interno del sistema codicistico di rito, le situazioni che prevedibilmente si sarebbero potute creare allorché la captazione avesse riguardato attività istituzionale svolta da personale dei servizi nell'espletamento delle funzioni istituzionali loro assegnate dalla legge nr. 124 *cit.*, che ha integralmente sostituito e riorganizzato i servizi segreti italiani in luogo della precedente legge del 1977, la nr. 801. È in tale ambito concettuale e normativo che viene elaborato l'oggi vigente art. 270-*bis* del Codice di procedura penale. In buona sostanza l'autorità giudiziaria, quando abbia acquisito, tramite intercettazioni, comunicazioni di servizio di appartenenti al DIS ovvero all'AISE o all'AISI deve disporre l'immediata secretazione la custodia in luogo protetto i documenti, e i supporti degli atti concernenti tali comunicazioni.

Terminate le intercettazioni, l'autorità giudiziaria trasmette al Presidente del Consiglio dei ministri copia della documentazione contenente le informazioni di cui intende avvalersi nel processo per accertare se talune di queste informazioni sia coperta da segreto di Stato. Prima della risposta del Presidente del Consiglio dei ministri le informazioni ad esso inviate possono essere utilizzate solo se vi è pericolo di inquinamento delle prove o pericolo di fuga, o quando è necessario intervenire per prevenire o interrompere la commissione di un delitto per il quale sia prevista la pena della reclusione non inferiore nel massimo a quattro anni. Resta ferma la disciplina concernente la speciale causa di giustificazione prevista per attività del personale dei servizi di informazione per la sicurezza⁽²¹³⁾.

⁽²¹²⁾ Ci s'intende riferire alle disposizioni organizzative, alle garanzie funzionali, allo stato giuridico del personale e alle norme di contabilità disciplinate dagli artt. 9 e seg. della citata legge nr. 124 che, al termine del percorso normativo, traccia la disciplina del segreto di Stato agli artt. 3, 9, 42.

⁽²¹³⁾ Le procedure di autorizzazione delle condotte previste dalla legge come reato, l'opposizione della speciale causa di giustificazione all'autorità giudiziaria e le disposizioni collegate all'ambito di applicazione delle garanzie funzionali in virtù delle quali il personale dei servizi segreti non è punibile allorquando pone in essere condotte previste dalla legge