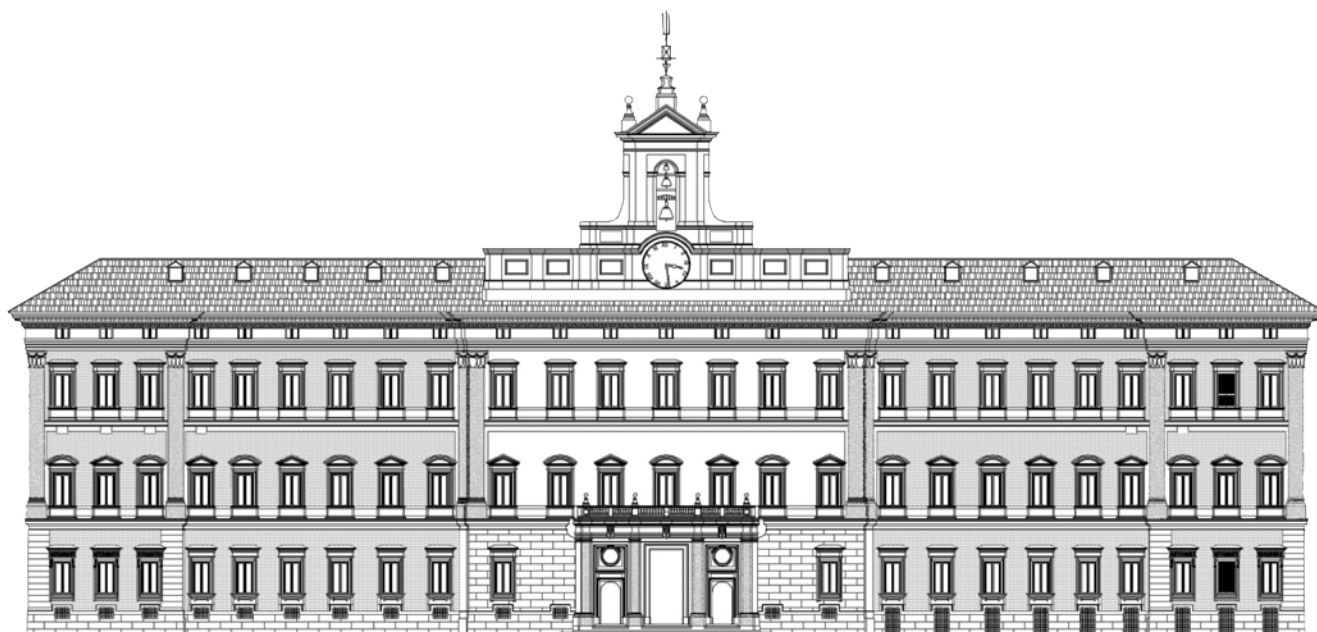




Camera dei deputati

XIX LEGISLATURA

Documentazione per l'esame di
Progetti di legge



Modifiche al codice di procedura penale in materia di sequestro di dispositivi, sistemi informatici o telematici o memorie digitali

A.C. 1822

Schede di lettura

n. 433

7 aprile 2025



Dipartimento Giustizia

Tel. 06 6760-9148 - ✉ st_giustizia@camera.it – ✕ [@CD_giustizia](https://twitter.com/CD_giustizia)

Progetti di legge n. 433

La documentazione dei servizi e degli uffici della Camera è destinata alle esigenze di documentazione interna per l'attività degli organi parlamentari e dei parlamentari. La Camera dei deputati declina ogni responsabilità per la loro eventuale utilizzazione o riproduzione per fini non consentiti dalla legge. I contenuti originali possono essere riprodotti, nel rispetto della legge, a condizione che sia citata la fonte.

gi0070.docx

INDICE

SCHEDE DI LETTURA	1
▪ Articolo 1 (<i>Sequestro di dispositivi e sistemi informatici o telematici, memorie digitali, dati, informazioni, programmi, comunicazioni e corrispondenza informatica inviate e ricevute – art. 254-ter c.p.p.</i>)	3
▪ Articolo 2 (<i>Ulteriori modifiche al codice di procedura penale</i>).....	15
▪ Articolo 3 (<i>Modifica alle norme di attuazione, di coordinamento e transitorie del codice di procedura penale</i>).....	25
▪ Articolo 4 (<i>Disposizione transitoria</i>)	26
TESTO A FRONTE	27

Schede di lettura

Articolo 1

(Sequestro di dispositivi e sistemi informatici o telematici, memorie digitali, dati, informazioni, programmi, comunicazioni e corrispondenza informatica inviate e ricevute – art. 254-ter c.p.p.)

L'**articolo 1** introduce nel codice di procedura penale il nuovo articolo 254-ter, recando una specifica disciplina relativa al **sequestro di dispositivi e sistemi informatici o telematici, memorie digitali, dati, informazioni, programmi, comunicazioni e corrispondenza informatica** inviate e ricevute.

L'**articolo 1** interviene sul Libro III, Titolo III, Cap. III del codice di procedura penale relativo alla disciplina del sequestro probatorio, quale mezzo di ricerca della prova nell'ambito del procedimento penale.

Nello specifico, l'articolo in commento inserisce all'interno del codice di procedura penale il nuovo **art. 254-ter** rubricato "***Sequestro di dispositivi e sistemi informatici o telematici, memorie digitali, dati, informazioni, programmi, comunicazioni e corrispondenza informatica inviate e ricevute***".

Il **comma 1** del nuovo articolo 254-ter c.p.p. prevede una **riserva di giurisdizione**, ai sensi della quale, nel corso delle indagini preliminari, compete al **giudice per le indagini preliminari**, su richiesta del pubblico ministero, **disporre il sequestro di dispositivi e sistemi informatici o telematici o di memorie digitali**, con decreto motivato.

Ai sensi del comma 1 è possibile procedere con il predetto sequestro alle seguenti **condizioni**:

- i dispositivi, sistemi o memorie da sottoporre a sequestro devono risultare **necessari per la prosecuzione delle indagini** (tenendo conto delle circostanze di tempo e di luogo del fatto e alle modalità della condotta);
- il rispetto del **criterio di proporzione**.

Il decreto che dispone il sequestro è immediatamente trasmesso, a cura della cancelleria del giudice per le indagini preliminari, al pubblico ministero che ne cura l'esecuzione.

Con specifico riferimento al **criterio di proporzionalità** della misura, la Corte di Cassazione ha osservato come esso trovi applicazione nei confronti dell'istituto

del sequestro, a prescindere dalle finalità perseguite (quindi sia cautelari, come nel caso del sequestro preventivo, sia probatorie, come nel caso del **sequestro probatorio**). Infatti, ad avviso dei giudici di legittimità, “la ragione posta a fondamento di un tale principio (essenzialmente rapportabile alla necessità di evitare limitazioni alla proprietà privata che non siano strettamente conseguenti alla finalità istituzionalmente perseguita dalla misura) deve valere indipendentemente dai fini cui il sequestro è diretto [...], essendo strettamente collegato all'elemento, comune a tutte tali ipotesi, della componente invasiva nell'altrui sfera personale attinente al diritto di disporre liberamente dei propri beni” (SS.UU. pen. sent. n. 36072 del 27 luglio 2018).

Il successivo **comma 2** del nuovo art. 254-ter c.p.p. prevede che il pubblico ministero possa curare personalmente **l'esecuzione del sequestro**, oppure **delegare** gli ufficiali di polizia giudiziaria a compiere tale operazione. In ogni caso, il sequestro è eseguito con **modalità tecniche idonee** a evitare l'alterazione o la perdita dei dati e, a tal fine, il pubblico ministero adotta le misure tecniche necessarie o impartisce specifiche prescrizioni.

È previsto che copia del decreto di sequestro è consegnata all'interessato, se presente.

➤ **Revoca del sequestro**

Il **comma 3** del nuovo art. 254-ter c.p.p. disciplina le ipotesi di **revoca del sequestro** disposto ai sensi del comma 1 del medesimo articolo.

La disposizione prevede che il sequestro sia immediatamente revocato, quando risultino **mancanti**, anche per fatti sopravvenuti, **le condizioni prescritte** dal comma 1. La revoca viene disposta dal pubblico ministero con decreto motivato, notificato a coloro che hanno diritto di promuovere impugnazione.

Se vi è istanza di revoca promossa dall'interessato, il pubblico ministero, quando ritiene che essa vada anche soltanto in parte respinta, la trasmette al giudice. Il pubblico ministero è tenuto a presentare al giudice richieste specifiche, nonché gli elementi sui quali fonda le proprie valutazioni. La richiesta di revoca deve essere trasmessa dal pubblico ministero al giudice non oltre il giorno successivo a quello del deposito nella segreteria.

➤ **Sequestro in situazione d'urgenza**

Il **comma 4** del nuovo art. 254-ter c.p.p. disciplina il sequestro di dispositivi in caso d'**urgenza**, ovvero quando vi sia una situazione d'urgenza tale per cui non sia possibile attendere il provvedimento del giudice. In tal caso, il sequestro è disposto con **decreto motivato dal pubblico ministero**.

Negli stessi casi di urgenza, prima dell'intervento del pubblico ministero, possono procedere al sequestro gli **ufficiali di polizia giudiziaria**, i quali, nelle **quarantotto ore successive**, trasmettono il verbale al pubblico ministero del luogo in cui il sequestro è stato eseguito.

Se il pubblico ministero non dispone la restituzione delle cose sequestrate, è tenuto a richiedere al giudice la **convalida** della misura di ricerca della prova adottata, e l'emissione del decreto di cui al comma 1.

In tal caso, il pubblico ministero è tenuto a trasmettere la predetta richiesta al giudice per le indagini preliminari **entro quarantotto ore**, rispettivamente:

- dal sequestro, nel caso di misura disposta direttamente dal pubblico ministero;
- dalla ricezione del verbale, nel caso in cui il sequestro sia stato effettuato dalla polizia giudiziaria.

Il **comma 5** prevede che il sequestro **perda efficacia**, qualora:

- non vengano rispettati i termini di cui al precedente comma 4;
- il giudice non emetta **ordinanza di convalida entro 10 giorni** dalla ricezione della richiesta del pubblico ministero.

Il medesimo comma 5, inoltre, precisa che copia dell'ordinanza di convalida adottata dal giudice deve essere **immediatamente notificata** alla persona alla quale le cose sono state sequestrate.

➤ **Duplicazione dei dispositivi, dei sistemi informatici o telematici o delle memorie digitali sequestrati**

Il **comma 6** del nuovo art. 254-ter c.p.p. stabilisce che il pubblico ministero, **entro cinque giorni** dal deposito del verbale di sequestro, avvisi degli aspetti concernenti il **conferimento dell'incarico** (giorno, ora e luogo) **per la duplicazione** dei dispositivi, sistemi o memorie che formano oggetto di sequestro, nonché della **facoltà di nominare consulenti tecnici** di parte, i seguenti soggetti:

- la persona sottoposta alle indagini;
- la persona alla quale le cose sono state sequestrate;
- la persona che avrebbe diritto alla loro restituzione;

- la persona offesa dal reato;
- i difensori dei soggetti summenzionati.

Il medesimo comma 6 precisa che è facoltà del pubblico ministero disporre la duplicazione anche dei dati, delle informazioni o dei programmi **accessibili da remoto** dal dispositivo in sequestro.

Peraltro, la disposizione prevede tempi stringenti per lo svolgimento delle operazioni tecniche: tra l'avviso (che, come si è detto, deve avvenire entro cinque giorni dal deposito del verbale di sequestro) e la data fissata per il conferimento dell'incarico non può intercorrere infatti un termine superiore a **dieci giorni**.

Si prevede inoltre l'applicazione della disposizione di cui all'art. 364, comma 2, c.p.p. che prevede di dare avviso alla persona sottoposta alle indagini preliminari dell'**assistenza tecnica d'ufficio**, qualora sia sprovvista di un difensore di fiducia. L'indagato ha comunque facoltà di nominare un difensore di fiducia.

A norma del **comma 7** del nuovo art. 254-ter c.p.p., il pubblico ministero, se richiesto, può autorizzare i soggetti che sono legittimati a prender parte all'attività di conferimento dell'incarico (v. *supra*), nonché i consulenti tecnici, se nominati, a **partecipare a distanza** al conferimento dell'incarico.

Il **comma 8**, invece, chiarisce che i difensori delle parti e i consulenti tecnici eventualmente nominati, oltre al conferimento dell'incarico, hanno **diritto di partecipare allo svolgimento delle operazioni di duplicazione** e di formulare osservazioni e riserve.

Ai sensi del **comma 9** le operazioni di duplicazione devono assicurare la **conformità** del duplicato **all'originale**, nonché la **sua immodificabilità**. A tal fine, è prescritto l'utilizzo di adeguati supporti informatici.

Per quanto concerne l'**attività di duplicazione** la Corte di Cassazione si è pronunciata su alcuni aspetti essenziali della procedura. Innanzitutto, i giudici di legittimità hanno asserito che la predetta procedura rappresenta quella più adeguata "a garantire l'integrità dei dati", in quanto la creazione di una copia-clonazione dell'*hard disk* conforme all'originale assicura l'immodificabilità dei dati stessi. In particolare, precisa la Corte, "il dato informatico, in quanto elemento dematerializzato e indipendente dal supporto, può essere sottoposto a sequestro a prescindere dal supporto stesso dove è incorporato. E tuttavia, una volta creata la c.d. copia originale, essa non rileva in sé come cosa pertinente al reato in quanto essa contiene un insieme di dati indistinti e magmatici rispetto ai quali **nessuna funzione selettiva è stata compiuta** al fine di verificare il nesso di strumentalità tra res, reato ed esigenza probatoria. La c.d. **copia integrale**, cioè, contiene

l'insieme dei dati contenuti nel contenitore (pc., tablet, telefono) **ma non soddisfa affatto l'esigenza indifferibile di porre sotto sequestro solo il materiale digitale che sia pertinente rispetto al reato per cui si procede** e che svolga una necessaria funzione probatoria. Ne deriva, come è stato specificato dalla Corte di cassazione, che la c.d. copia integrale costituisce solo una **copia - mezzo**, cioè una copia che consente di restituire il contenitore, ma che non legittima affatto il trattenimento dell'insieme di dati appresi” (Cass. pen. sent. n. 34265 del 2 dicembre 2020).

Fatti salvi i casi di revoca del decreto motivato che dispone il sequestro probatorio, il pubblico ministero, una volta conclusa l'attività di duplicazione, dispone senza ritardo la **restituzione dei dispositivi, sistemi o memorie digitali sequestrati** all'avente diritto.

Tuttavia, non si fa luogo alla restituzione, qualora occorre mantenere il sequestro per finalità preventive di cui all'art. 321 c.p.p. (**comma 11**).

Si ricorda che il cd. **sequestro preventivo** di cui all'art. 321 c.p.p. è disposto con decreto motivato dal giudice competente per il merito ovvero dal giudice per le indagini preliminari (qualora venga disposto durante le indagini preliminari), su richiesta del pubblico ministero, laddove vi sia “pericolo che la libera disponibilità di una cosa pertinente al reato possa aggravare o protrarre le conseguenze di esso ovvero agevolare la commissione di altri reati”.

➤ **Deroghe alla normale procedura di duplicazione**

A norma del **comma 10** del nuovo art. 254-ter c.p.p. l'attività di duplicazione può avvenire **in deroga** al disposto dei **commi 6, 7 e 8**, sempre con modalità tecniche idonee ad assicurare la conformità del duplicato all'originale e la sua immodificabilità, al ricorrere di una delle seguenti condizioni:

- nei procedimenti di cui agli **articoli 406, comma 5-bis c.p.p.** (si tratta dei procedimenti per taluno dei delitti indicati nell'articolo 51, comma 3-bis c.p.p. e nell'articolo 407, comma 2, lett. a), nn. 4 e 7-bis, c.p.p.)¹;

¹ Si ricorda che i reati di cui agli artt. 51, co. 3-bis c.p.p. e 407, co. 2, lett. a), nn. 4 e 7-bis, c.p.p. rappresentano fattispecie connotate da una particolare offensività, nonché rilevanza sociale. In particolare, l'art. 51 c.p.p. al co. 3-bis, prevede una serie di delitti associativi, consumati o tentati, diretti a commettere determinati fatti di reato, tra cui: a) reati contro la personalità individuale come “riduzione o mantenimento in schiavitù” (art. 600 c.p.), “tratta di persone” (art. 601 c.p.), “traffico di organi prelevati da persona vivente” (art. 601-bis c.p.) e “acquisto e alienazione di schiavi” (art. 602 c.p.); b) reati contro la personalità individuale in danno a soggetti minorenni, tra cui “prostituzione minorile” (art. 600-bis c.p.), “pornografia minorile” (art. 600-ter c.p.); c) reati contro la libertà sessuale tra cui “violenza sessuale” (art. 609-bis c.p.), “atti sessuali con minorenni” (art. 609-quater c.p.), “violenza sessuale di gruppo” (art. 609-octies c.p.); d) reati associativi in materia di immigrazione clandestina, commessi al fine di realizzare tassative ipotesi delittuose. Invece, l'407 c.p.p. al co. 2, lett. a), nn. 4 e 7-bis, c.p.p.

- nei procedimenti di cui **all'art. 371-bis, comma 4-bis c.p.p.** (si tratta dei procedimenti per i delitti di cui agli articoli 615-ter, comma 3, 635-ter e 635-quinquies c.p.², nonché, quando i fatti sono commessi in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità, dei procedimenti per i delitti di cui agli articoli 617-quater, 617-quinquies e 617-sexies c.p.)³;
- quando sussiste un pericolo per la vita o l'incolumità di una persona o la sicurezza dello Stato, ovvero un pericolo di concreto pregiudizio per le indagini in corso, o un pericolo attuale di cancellazione o dispersione dei dati, delle informazioni o dei programmi.

Con riferimento alle prime due ipotesi (procedimenti indicati dall'art. 406, comma 5-bis c.p.p. e procedimenti di cui all'art. 371-bis, comma 4-bis c.p.p.) al ricorrere della quale si prevede la possibilità per il pubblico ministero di procedere all'attività di duplicazione "in deroga alle previsioni di cui ai commi 6, 7 e 8 del nuovo art. 254-ter c.p.p.", si ricorda che la Corte costituzionale (**sent. n. 139 del 2010**) ha affermato che «le presunzioni assolute, specie quando limitano diritti fondamentali della persona, violano il principio di uguaglianza se sono arbitrarie e irrazionali, non rispondendo a dati di esperienza generalizzati, riassunti nella formula dell'*id quod plerunque accidit*», sottolineando come il riferimento ad un determinato reato o a una categoria di reati non può essere idoneo *ex se* a fornire dati di esperienza generalizzati in ordine alla sintomaticità di una fattispecie a mettere in pericolo la sicurezza o l'efficienza del processo (**sent. n. 185 del 2015**).

➤ **Analisi del duplicato e sequestro dei dati, informazioni o programmi pertinenti al reato**

Effettuata l'analisi del duplicato informatico, il pubblico ministero dispone con decreto motivato il sequestro dei dati, delle informazioni e dei

prevede fattispecie che destano un particolare allarme sociale, tra cui: a) delitti commessi per finalità di terrorismo o di eversione dell'ordinamento costituzionale con un trattamento sanzionatorio particolarmente gravoso; b) reati contro la libertà personale e la libertà sessuale particolarmente offensivi.

² Nello specifico, l'art. 615-ter, co. 3, c.p. sanziona l'accesso abusivo ad un sistema informatico o telematico di interesse militare ovvero rilevante per l'ordine pubblico, per la sicurezza pubblica per la sanità o per la protezione civile, o, comunque, di interesse pubblico. L'art. 635-ter c.p. reprime le condotte di danneggiamento di informazioni, dati e programmi informatici pubblici o di interesse pubblico. L'art. 635-quinquies, invece, punisce i delitti di danneggiamento di sistemi informatici o telematici di pubblico interesse.

³ Nel dettaglio, l'art. 617-quater c.p. sanziona le condotte di colui che fraudolentemente intercetta, impedisce o interrompe comunicazioni informatiche o telematiche. L'art. 617-quinquies c.p. reprime i reati di detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche. L'art. 617-sexies c.p., infine, punisce colui che falsifica, altera o sopprime il contenuto di comunicazioni informatiche o telematiche.

programmi **strettamente pertinenti al reato** in relazione alle circostanze di tempo e di luogo del fatto e alle modalità della condotta, nel rispetto dei criteri di necessità e proporzione (**comma 12, primo periodo**).

Sul punto, la Suprema Corte ha specificato che la misura del sequestro probatorio di materiale informatico “è consentita a condizione che il sequestro **non assuma una valenza meramente esplorativa**” e che la disposizione di un **sequestro esteso ed omnicomprendente** deve essere **debitamente motivata** “in ragione del tipo di reato per cui si procede, della condotta e del ruolo attribuiti alla persona titolare dei beni, e della difficoltà di individuare *ex ante* l'oggetto del sequestro” (**Cass. pen. sent. n. 222 del 3 gennaio 2024**).

A tal riguardo, la Cassazione ha ulteriormente asserito che costituisce “un principio ormai consolidato (...) che l'estrazione di copia integrale dei dati in essi contenuti, che consente la restituzione del dispositivo, **non legittima il trattenimento della totalità delle informazioni apprese oltre il tempo necessario a selezionare quelle pertinenti al reato per cui si procede**, sicché il pubblico ministero è tenuto a predisporre un'adeguata organizzazione per compiere tale selezione nel tempo più breve possibile”. In particolare, spetterà al giudice verificare se le operazioni di selezione del materiale siano conformi all'esigenza di differimento temporaneo della valutazione del **nesso di pertinenzialità tra res e reato** che si vuole accertare ovvero si traducano in una elusione delle garanzie dell'interessato, con conseguente violazione **del diritto di proporzione** e limitazione illegittima di diritti delle persone (**Cass. Pen. sent. n. 50009 del 04 ottobre 2023**).

Inoltre, la Suprema Corte di Cassazione rileva che “coerentemente con l'estensione anche alle misure reali dei requisiti di adeguatezza e proporzionalità, è stato condivisibilmente ritenuto illegittimo il sequestro a fini probatori di un dispositivo elettronico che conduca, in difetto di specifiche ragioni, alla indiscriminata apprensione di una massa di dati informatici, senza alcuna previa selezione di essi e comunque senza l'indicazione degli eventuali criteri di selezione” (**Cass. pen. sent. n. 17312 del 24 aprile 2024**).

Alla luce dei principi di diritto appena richiamati, si valuti l'opportunità di introdurre un termine entro cui il pubblico ministero deve compiere l'attività di selezione dei dati, delle informazioni e dei programmi ritenuti strettamente pertinenti al reato e la conseguente adozione del decreto motivato di sequestro.

Il **secondo periodo del comma 12** prende in esame il sequestro probatorio dei dati inerenti a **comunicazioni, conversazioni o corrispondenza informatica** inviate e ricevute.

In tal caso, il pubblico ministero formula apposita **richiesta nei confronti del giudice per le indagini preliminari**, che provvede con decreto motivato a disporre il sequestro, allorquando ricorrano le condizioni

richieste dal primo periodo dello stesso comma 12 (ovvero si tratti di dati, informazioni e programmi strettamente pertinenti al reato), nonché i presupposti prescritti agli articoli 266, comma 1 (relativo ai limiti di ammissibilità delle intercettazioni)⁴, e 267, comma 1 c.p.p. (inerente ai presupposti ed alle forme del provvedimento che dispone le intercettazioni)⁵.

Sul punto merita di essere segnalata la **sentenza n. 170 del 2023** mediante cui la Corte costituzionale ha accolto il conflitto di attribuzione promosso dal Senato nei confronti della Procura della Repubblica presso il Tribunale di Firenze, nella parte in cui era diretto a contestare la legittimità dell'acquisizione di corrispondenza di un senatore in violazione dell'art. 68, comma 3, Cost., che impone il rilascio della preventiva autorizzazione, da parte della Camera di appartenenza, al fine di sottoporre il parlamentare ad intercettazione. In particolare, la Consulta con la predetta pronuncia ha ricondotto all'interno della nozione di **"corrispondenza" ex art 15 Cost. i messaggi di posta elettronica e WhatsApp, in particolare quelli già ricevuti e letti dal destinatario, ma**

⁴ Si ricorda che l'art. 266, co. 1, c.p.p. prevede un elenco tassativo di reati per i quali è possibile procedere ad intercettazione di conversazioni o comunicazioni telefoniche, nonché di altre forme di comunicazioni. In particolare, le ipotesi sono le seguenti: a) delitti non colposi per i quali è prevista la pena dell'ergastolo o della reclusione superiore nel massimo a cinque anni determinata a norma dell'articolo 4 c.p.p.; b) delitti contro la pubblica amministrazione per i quali è prevista la pena della reclusione non inferiore nel massimo a cinque anni determinata a norma dell'articolo 4; c) delitti concernenti sostanze stupefacenti o psicotrope; d) delitti concernenti le armi e le sostanze esplosive; e) delitti di contrabbando; f) reati di ingiuria, minaccia, usura, abusiva attività finanziaria, abuso di informazioni privilegiate, manipolazione del mercato, molestia o disturbo alle persone col mezzo del telefono; f-bis) delitti legati alla diffusione, divulgazione, distribuzione e pubblicizzazione di materiale pornografico minorile, nonché la divulgazione o la distribuzione di notizie per l'adescamento di minori (art. 600-ter, comma 3 c.p.), nonché il delitto di adescamento di minori di cui all'art. 609-undecies c.p.; f-ter) i delitti di: commercio di sostanze alimentari nocive (art. 644 c.p.), contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni (art. 473 c.p.), introduzione nello Stato e commercio di prodotti con segni falsi (art. 474 c.p.), frode nell'esercizio del commercio (art. 515 c.p.), vendita di sostanze alimentari non genuine come genuine (art. 516 c.p.), contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari (art. 517-quater), invasione di terreni o edifici (art. 633 c.p.); f-quater) il delitto di atti persecutori (art. 612-bis c.p.); f-quinquies) delitti commessi avvalendosi delle condizioni previste dal reato di associazione di stampo mafioso anche straniera (art. 416-bis c.p.) ovvero al fine di agevolare l'attività della predetta associazione.

⁵ L'art. 267, co. 1 c.p.p. stabilisce che, nei limiti previsti dall'art. 266 c.p.p. il PM richiede al GIP l'autorizzazione a disporre le operazioni di intercettazione. L'autorizzazione è concessa dal giudice con decreto motivato al ricorrere dei seguenti presupposti: a) la presenza di gravi indizi di reato; b) l'assoluta indispensabilità ai fini della prosecuzione delle indagini. Il decreto che autorizza l'intercettazione tra presenti mediante inserimento di captatore informatico su dispositivo elettronico portatile, deve dare conto delle ragioni che, nel caso di specie, hanno determinato il ricorso a tale modalità di svolgimento delle intercettazioni. Il decreto motivato deve, inoltre, indicare i luoghi e il tempo, anche indirettamente determinati, in relazione ai quali è consentita l'attivazione del microfono. Queste ultime indicazioni non devono essere enunciate qualora si proceda per particolari fatti di reato previsti dalla stessa norma.

conservati nella memoria dei dispositivi elettronici del destinatario stesso o del mittente.

Nello specifico, secondo quanto affermato dai giudici costituzionali, “degradare la comunicazione a mero documento quando non più *in itinere*” finirebbe per non rendere più configurabile l’applicazione della tutela apprestata dall’art. 15 Cost. nei confronti delle “comunicazioni operate tramite posta elettronica e altri servizi di messaggistica istantanea, in cui all’invio segue immediatamente – o, comunque sia, senza uno iato temporale apprezzabile – la ricezione”.

Il **terzo periodo del comma 12** prende in esame la fattispecie disciplinata dall’art. 13 del D.L. 152 del 1991, il quale regola lo svolgimento di intercettazioni di conversazioni o comunicazioni in relazione “ad un delitto di criminalità organizzata o di minaccia col mezzo del telefono in ordine ai quali sussistano sufficienti indizi”.

Si ricorda che il richiamato art. 13 opera in deroga all’art. 267 c.p.p., prevedendo, per le fattispecie ricordate, la possibilità di disporre l’intercettazione con decreto motivato del giudice per le indagini preliminari, quando essa sia “**necessaria per lo svolgimento delle indagini**” e siano presenti “**sufficienti indizi**” di reato, laddove l’art. 267 c.p.p. prevede la possibilità di ricorrere a intercettazioni quando ciò “è assolutamente indispensabile ai fini della prosecuzione delle indagini”.

Ciò premesso, il terzo periodo del comma 12 consente il sequestro probatorio nei procedimenti per i quali trova applicazione il citato articolo 13 del decreto-legge n. 152 del 1991, al ricorrere dei presupposti richiesti dal medesimo articolo 13.

Infine, si prevede che copia del decreto motivato con il quale si dispone il sequestro dei dati, delle informazioni e/o dei programmi sia notificata all’avente diritto alla restituzione del dispositivo (**comma 12, ultimo periodo**).

Ai sensi del **comma 13**, i dati, le informazioni e i programmi sottoposti a sequestro, con le modalità sopra descritte ex comma 12, sono riversati su idonei supporti con modalità tecniche idonee ad assicurare la loro conformità ai medesimi dati, informazioni e programmi contenuti nel duplicato e la loro immodificabilità. I predetti supporti sono acquisiti al fascicolo.

Il **comma 14** stabilisce che in materia di sequestro di dati, informazioni e programmi, comunicazioni o conversazioni trovino applicazione le seguenti disposizioni in quanto compatibili:

- art. 103 c.p.p. in materia di garanzie di libertà del difensore;
- art. 269, commi 2 e 3 c.p.p., in materia di conservazione e distruzione delle registrazioni di comunicazioni o conversazioni intercettate;
- art. 270, commi 1, 2 e 3 c.p.p., in materia di limiti all'utilizzazione dei risultati delle intercettazioni;
- art. 270-bis c.p.p. che regola le comunicazioni di servizio di appartenenti al Dipartimento delle informazioni per la sicurezza ed ai servizi di informazione per la sicurezza;
- art. 271 c.p.p. inerente ai divieti di utilizzazione dei risultati ottenuti a seguito di intercettazione.

➤ **Sequestro di dispositivi, sistemi o memorie digitali, nonché di dati, informazioni o comunicazioni dopo l'esercizio dell'azione penale**

Il **comma 15 del nuovo art. 254-ter c.p.p.** prende in considerazione l'ipotesi in cui si proceda al sequestro dei supporti di cui al comma 1 e dei dati di cui al comma 12 in un momento successivo rispetto all'esercizio dell'azione penale da parte del pubblico ministero.

In tal caso, salve le ipotesi di cui all'art. 419 comma 3 (il quale prescrive che l'avviso mediante cui si notificano le parti dello svolgimento dell'udienza preliminare deve contenere, tra gli altri, anche "l'invito a trasmettere la documentazione relativa alle indagini eventualmente espletate dopo la richiesta di rinvio a giudizio"), il decreto motivato che dispone il sequestro viene adottato dal giudice che procede. Inoltre, alla duplicazione del supporto informatico si procede con il mezzo di prova della **perizia**.

➤ **Conservazione e distruzione del duplicato informatico**

I **commi 16 e 17** disciplinano, rispettivamente, gli istituti della **conservazione** e della **distruzione del duplicato informatico**.

E' previsto che la **conservazione** del duplicato informatico avvenga presso la procura della Repubblica, in un luogo protetto da specifiche misure di sicurezza, con modalità tali da assicurare l'assoluta riservatezza, **sino alla sentenza o al decreto penale di condanna non più soggetti impugnazione**.

Tuttavia, gli interessati possono chiedere al giudice che ha disposto o convalidato il sequestro, a tutela della propria riservatezza, la **distruzione del duplicato**, quando i dati, le informazioni o i programmi non sono necessari per il procedimento.

Tale decisione viene assunta dal giudice competente in camera di consiglio secondo quanto disposto dall'art. 127 c.p.p.

Nel caso in cui vi sia **l'archiviazione**, la distruzione viene immediatamente disposta dal giudice, salvo che, anche su richiesta di uno dei soggetti previsti dall'art. 409 comma 2 c.p.p. (pubblico ministero, indagato e persona offesa), ritenga sussistenti specifiche esigenze che ne impongono la conservazione.

Il **comma 18** prescrive che nei casi in cui è prevista la distruzione del duplicato informatico, essa debba avvenire sotto controllo del giudice e dell'operato debba essere redatto verbale.

Si ricorda che il duplicato informatico realizza una cd. copia-mezzo contenente l'integrale mole di dati ed informazioni contenuti all'interno del dispositivo originale. Tuttavia, come osservato in precedenza (v. *supra*, paragrafo “Analisi del duplicato e sequestro dei dati, informazioni o programmi pertinenti al reato”), sebbene la cd. copia forense consente la restituzione all'interessato del dispositivo originale, tuttavia, ad avviso della Corte di Cassazione, non è legittimo “il trattenimento della totalità delle informazioni apprese oltre il tempo necessario a selezionare quelle pertinenti al reato per cui si procede” (v. **Cass. pen. sent. n. 34265 del 2 dicembre 2020**). Pertanto, i giudici di legittimità precisano che il pubblico ministero è tenuto ad illustrare: a) la necessità di un sequestro esteso ed omnicomprensivo ovvero le specifiche informazioni oggetto di ricerca; b) i parametri di selezione di dati di interesse; c) “i tempi entro cui verrà effettuata tale selezione **con conseguente restituzione anche della copia informatica dei dati non rilevanti**” (Cass. pen. sent. n. 17312 del 24 aprile 2024, in termini sostanzialmente analoghi anche Cass. pen. n. 50009 del 15 dicembre 2023, secondo cui una volta compiuta l'attività di selezione delle informazioni/dati da sottoporre a sequestro, il pubblico ministero deve provvedere “alla restituzione della copia integrale agli aventi diritto”).

Inoltre, le **Sez. Unite** della Cassazione con la sentenza **n. 40963 del 7 settembre 2017**, affrontando la questione inerente alla legittimità del sequestro disposto su strumenti informatici, hanno posto l'attenzione sul caso in cui il “documento (...) informatico o di altro tipo, trasferisca il proprio valore anche sulla copia, venendo così in gioco l'interesse alla disponibilità esclusiva del patrimonio informativo. È indubbio che, in tali casi, la restituzione [del dispositivo sequestrato] non può considerarsi risolutiva, dal momento che la mera reintegrazione nella disponibilità della cosa non elimina il pregiudizio, conseguente al mantenimento del vincolo sugli specifici contenuti rispetto al contenitore, incidente su **diritti certamente meritevoli di tutela, quali quello alla riservatezza o al segreto**”.

*Alla luce di quanto sopra esposto si valuti l'opportunità di prevedere, previo coordinamento con le disposizioni di cui alle lett. o), q), r) del successivo **articolo 2**, le modalità di restituzione all'interessato del*

duplicato informatico, contenente l'insieme integrale dei dati contenuti nel dispositivo originale.

➤ **Riesame dei provvedimenti di sequestro**

Il **comma 19** ammette la possibilità di esperire la procedura di **riesame** ai sensi dell'art. 257 c.p.p. (rubricato "riesame del decreto di sequestro") avverso i provvedimenti di sequestro e di convalida dello stesso di cui ai precedenti commi 1, 4 e 12.

L'art. 257 c.p.p. stabilisce, in via generale, che, contro il decreto che dispone il sequestro probatorio l'imputato, la persona alla quale le cose sono state sequestrate e quella che avrebbe diritto alla loro restituzione possono proporre richiesta di riesame, anche nel merito, secondo le norme che regolano l'impugnazione dei provvedimenti di sequestro conservativo e sequestro preventivo, quali misure cautelari reali (v. art. 324 c.p.p.).

Articolo 2 (Ulteriori modifiche al codice di procedura penale)

L'articolo 2 apporta una serie di **modifiche al codice di procedura penale** in materia di: perquisizione informatica e sequestro conseguente alla perquisizione; divieto di pubblicazione del contenuto dei duplicati; perquisizioni, accertamenti urgenti e sequestri d'iniziativa della polizia giudiziaria; fasi successive al sequestro informatico.

La **lett. a)** del comma 1 modifica il **comma 2-bis dell'articolo 114 c.p.p.** ed è volta ad introdurre un **divieto di pubblicazione** con il mezzo della stampa o con altro mezzo di diffusione del **contenuto dei duplicati** formati ai sensi dell'art. 254-ter, come introdotto dal precedente articolo 1, **diversi dai dati, dalle informazioni e dai programmi sequestrati** ai sensi del comma 12 del medesimo articolo 254-ter

La disposizione distingue, pertanto, il regime di pubblicabilità del duplicato informatico (vale a dire della copia integrale del contenuto del dispositivo sequestrato) da quello previsto per il materiale successivamente selezionato e sequestrato dal pubblico ministero, limitando al primo l'applicazione del divieto di pubblicazione anche parziale del contenuto. Con riferimento ai dati, alle informazioni e ai programmi sequestrati troverà, invece, applicazione la disciplina generale contenuta nell'art. 114 c.p.p.

Si segnala che la novella è costruita sul testo del comma 2-bis dell'articolo 114 c.p.p. antecedente la modifica operata dall'art. [2, comma 1, lett. b\), della legge 9 agosto 2024, n. 114](#), che limita il divieto di **pubblicazione, anche parziale**, del contenuto delle intercettazioni ai casi in cui il contenuto **non sia riprodotto dal giudice nella motivazione di un provvedimento o utilizzato nel corso del dibattimento**.

Si valuti l'esigenza di coordinare la novella prevista dall'art. 2, lett. a), della proposta di legge con la vigente formulazione del comma 2-bis dell'art. 114 c.p.p.

Perquisizione informatica e sequestro conseguente alla perquisizione

Un secondo gruppo di novelle incide sulla disciplina della **perquisizione informatica** attraverso una serie di modifiche ad alcune disposizioni del codice di procedura penale.

Anzitutto, si interviene sul comma 1-bis dell'articolo 247 c.p.p. che **disciplina i casi e le forme della perquisizione informatica**, al fine di

ricomprendere i dispositivi e le memorie digitali nel novero dei possibili “oggetti” di natura informatica dell’attività di perquisizione (**lett. c**).

Il comma 1-*bis* dell'articolo 247 c.p.p. nella sua formulazione vigente prevede il ricorso alla perquisizione allorquando vi sia fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico. A tal fine, la disposizione prevede l’adozione di misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l’alterazione.

Viene altresì introdotto, nel codice di rito, il **nuovo articolo 250-bis**, che detta una specifica disciplina per le **perquisizioni di sistemi informatici o telematici o memorie digitali** (**lett. d**).

Il nuovo articolo 250-*bis* stabilisce che, **quando è disposta la perquisizione informatica** ai sensi dell’art. 247, comma 1-*bis*, c.p.p. all'atto di iniziare le operazioni, all'imputato, se presente, e a chi abbia l'attuale disponibilità del sistema informatico o telematico, del dispositivo o della memoria digitale deve essere:

- consegnata una **copia del decreto di perquisizione**;
- dato **avviso** della facoltà di farsi rappresentare o assistere da **persona di fiducia**, purché questa sia prontamente reperibile e idonea a norma dell'articolo 120 c.p.p.;
- al solo imputato presente, dato avviso della facoltà di farsi assistere da **un consulente tecnico**, purché questo sia prontamente reperibile.

In assenza dell’imputato o di chi ha la disponibilità del sistema informatico o telematico, del dispositivo o della memoria digitale, la copia del decreto di perquisizione è consegnata e l'avviso della facoltà di farsi rappresentare o assistere da persona di fiducia, è rivolto a un congiunto, un coabitante o un collaboratore.

Connessa alla modifica da ultimo descritta è quella che interviene **sull’articolo 233 c.p.p.**, il quale disciplina la **consulenza tecnica extraperitale** (**lett. b**).

Si tratta, come noto, di un mezzo di prova che può essere introdotto dalle parti nel procedimento quando non sia disposta la perizia. In particolare, l'articolo 233 c.p.p. prevede una serie di attività di indagine esercitabili dall'esperto di parte lungo tutto l'arco procedimentale: ai sensi del comma 1-*bis* il consulente tecnico può essere autorizzato ad esaminare le cose sequestrate nel luogo in cui esse si trovano, ad intervenire alle ispezioni, ovvero ad esaminare l'oggetto delle ispezioni alle quali il consulente non è intervenuto. Si tratta di un'attività di esame

su cose sequestrate o già ispezionate che implica però una mera visione: il comma 1-ter dell'articolo 233 prevede infatti che il giudice impartisca le prescrizioni finalizzate a lasciare inalterato lo stato di cose e luoghi esaminati dal consulente tecnico nonché al rispetto delle persone.

La citata lett. b), introducendo il nuovo **comma 1-quater** nell'articolo 233 c.p.p., amplia le attività di indagine esercitabili dall'esperto ricomprendendovi anche la **facoltà di assistere**, senza preavviso, **alla perquisizione di un sistema informatico o telematico**, di un dispositivo o di una memoria digitale, potendo formulare osservazioni e riserve.

Il comma 1 dell'articolo 2 del provvedimento in esame introduce, inoltre, una disciplina di carattere generale destinata a trovare applicazione nei casi di **sequestro conseguente alla perquisizione informatica**.

A tal fine, vengono aggiunti **due ulteriori commi** (commi 1-bis e 1-ter) **all'articolo 252 c.p.p.**, il quale, nella sua formulazione vigente, prevede il sequestro del corpo del reato o delle cose pertinenti al reato, reperite nel corso di una perquisizione (**lett. e**).

Il **nuovo comma 1-bis** dell'art. 252 c.p.p. prevede che i dati, le informazioni o i programmi rinvenuti a seguito della perquisizione informatica, sono sottoposti a sequestro nel rispetto dei presupposti di cui all'articolo 254-ter, comma 12 (su cui v. *supra* scheda di lettura relativa all'art. 1). Viene anche in quest'ambito ribadita la differenziazione della procedura **a seconda della tipologia di elemento da acquisire**, vale a dire della natura comunicativa o meno dell'elemento.

Si prevede, infatti, che l'acquisizione dei dati, delle informazioni o dei programmi sottoposti a sequestro è in ogni caso effettuata ai sensi dell'articolo 254-ter, comma 13, ovvero sia attraverso il riversamento su idonei supporti, con modalità tecniche adeguate ad assicurarne l'immodificabilità e la conformità dei dati. Se i dati sono inerenti a **comunicazioni, conversazioni e corrispondenza informatica** inviate e ricevute, il pubblico ministero deve richiedere al giudice la **convalida e l'emissione del decreto di sequestro entro quarantotto ore** dall'esecuzione.

Il **nuovo comma 1-ter** dell'articolo 252 c.p.p. prevede inoltre che, quando a seguito della perquisizione informatica risulta necessario sottoporre a sequestro il dispositivo o il sistema informatico o telematico o la memoria digitale oggetto della perquisizione, si applica la disciplina del sequestro dettata dal nuovo articolo 254-ter e il pubblico ministero procede ai sensi del comma 4 dello stesso articolo. Ne discende che, **nei casi d'urgenza**, il pubblico ministero provvede con decreto motivato a disporre

il sequestro, per poi trasmettere, entro quarantotto ore gli atti al giudice per la convalida della misura adottata e l'emissione del decreto.

Perquisizioni, accertamenti urgenti e sequestri d'iniziativa della polizia giudiziaria

L'articolo 2 della proposta di legge in commento reca altresì modifiche all'**articolo 352 c.p.p.**, che disciplina le **perquisizioni informatiche a iniziativa della polizia giudiziaria**, eseguibili nei casi di flagranza del reato ovvero quando sussistono particolari ragioni di urgenza che non consentono di attendere l'intervento dell'autorità giudiziaria (**lett. l**).

Al ricorrere di tali ipotesi, il comma 1-bis dell'art. 352 c.p.p. prevede che gli ufficiali di polizia giudiziaria, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione, procedono alla perquisizione di sistemi informatici o telematici, ancorché protetti da misure di sicurezza, quando hanno fondato motivo di ritenere che in questi si trovino occultati dati, informazioni, programmi informatici o tracce comunque pertinenti al reato che possono essere cancellati o dispersi.

In particolare, la proposta di legge:

- modifica il comma 1-bis dell'art. 352 c.p.p. adeguando la formulazione testuale (che attualmente richiama solo i sistemi informatici o telematici) alla nuova disciplina introdotta: viene così inserito il riferimento anche ai “**dispositivi e alle memorie digitali**”;
- aggiunge un ulteriore periodo al comma 1-bis ai sensi del quale, in caso di perquisizione informatica, la polizia giudiziaria deve **avvisare l'indagato presente della facoltà di farsi assistere da un consulente tecnico**, purché questo sia prontamente reperibile;
- inserisce un **nuovo comma 1-ter**, a tenore del quale i dati, le informazioni o i programmi rinvenuti a seguito della perquisizione informatica sono sottoposti a sequestro nel rispetto dei presupposti di cui all'articolo 254-ter, comma 12. L'acquisizione dei dati, delle informazioni o dei programmi sottoposti a sequestro è in ogni caso effettuata ai sensi dell'articolo 254-ter, comma 13, ovvero sia attraverso il riversamento su idonei supporti, con modalità tecniche adeguate ad assicurarne l'immodificabilità e la conformità rispetto ai medesimi dati, informazioni e programmi contenuti nel duplicato.

Si valuti l'opportunità di inserire il riferimento a "dispositivi e memorie digitali" anche nell'articolo 244, comma 2, c.p.p., nella parte in cui disciplina l'ispezione informatica.

L'articolo in commento provvede, inoltre, a sostituire il secondo e il terzo periodo del comma 2 dell'**articolo 354 c.p.p.** in tema di **accertamenti urgenti informatici (lett. m)**.

Gli accertamenti urgenti informatici sono un tipo particolare di accertamento di **polizia giudiziaria** implicante il compimento di atti e operazioni tecniche equivalenti a quelli previsti nell'ambito degli altri mezzi di ricerca della prova digitale, ma caratterizzati dalla finalità di assicurare la conservazione dei dati, delle informazioni e dei programmi informatici o dei sistemi informatici o telematici e di impedirne l'alterazione e l'accesso prima che il pubblico ministero possa intervenire ovvero assuma la direzione delle indagini.

L'articolo 354 c.p.p. affida, peraltro, agli ufficiali di polizia giudiziaria il compito di provvedere, ove possibile, alla immediata duplicazione su adeguati supporti dei dati informatici, mediante una procedura che assicuri la conformità dei dati acquisiti a quelli originali e l'immodificabilità dei dati stessi.

Oltre ad inserire il **riferimento anche ai dispositivi e alle memorie digitali** tra i possibili oggetti dell'accertamento informatico, si prevede che, se del caso, quando il sequestro ha ad oggetto dati, informazioni o programmi informatici, gli ufficiali di polizia giudiziaria sequestrano il corpo del reato e le cose a questo pertinenti, osservando le disposizioni di cui all'articolo 352, comma 1-ter (su cui v. *supra*).

Viene, altresì, introdotto nell'art. 354 c.p.p. un **nuovo comma 2-bis**, ai sensi del quale, quando è necessario sottoporre a **sequestro un dispositivo, un sistema informatico o telematico o una memoria digitale**, si applicano le disposizioni di cui all'art. 254-ter c.p.p. e la polizia giudiziaria procede ai sensi del comma 4 del medesimo articolo. Ne discende che gli **ufficiali di polizia giudiziaria possono procedere al sequestro**, ma, nelle **quarantotto ore successive**, devono trasmettere il verbale al pubblico ministero del luogo in cui il sequestro è stato eseguito ai fini della convalida.

Attraverso le disposizioni di cui alla **lett. n)**, all'**articolo 355 c.p.p.**, che disciplina la **convalida del sequestro** e il suo **riesame**, viene aggiunto un ulteriore comma. Il nuovo **comma 2-bis** prevede che nel caso di **sequestro** eseguito ai sensi degli articoli 352, comma 1-ter, e 354, comma 2-bis (come inseriti dalle lettere *l)* e *m)* del comma 1 dell'articolo in commento, v. *supra*), avente ad oggetto dati inerenti a **comunicazioni, conversazioni e**

corrispondenza informatica inviate e ricevute, il pubblico ministero deve richiedere al **giudice la convalida e l'emissione del decreto di sequestro entro quarantotto ore dall'esecuzione**.

Altre forme di sequestro

L'articolo 2 reca, inoltre, modifiche alla disciplina di alcune forme particolari di sequestro.

Rilevano, in tal senso, le modifiche recate agli **articoli 254 e 254-bis c.p.p.**, che riguardano, rispettivamente:

- il sequestro, presso coloro che forniscono servizi postali, telegrafici, telematici o di telecomunicazioni, di documenti rientranti nella nozione di "corrispondenza" (per approfondimento in tema di sequestro di corrispondenza si veda il par. dell'articolo 1 "Analisi del duplicato e sequestro dei dati, informazioni o programmi pertinenti al reato", *supra*);
- il sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni.

Con riferimento al **sequestro di corrispondenza**, la novella all'art. 254 c.p.p. prevede che sia disposto dal giudice in presenza dei presupposti di cui all'articolo 254-ter, comma 12, salva la possibilità, nei casi di urgenza, di provvedere ai sensi del comma 4 del medesimo articolo. Viene, inoltre, stabilita l'applicabilità del comma 14 dell'articolo 254-ter, il quale a sua volta rinvia, in quanto compatibili, alle seguenti disposizioni: art. 103 c.p.p. in materia di garanzie di libertà del difensore; art. 269, commi 2 e 3, c.p.p., in materia di conservazione e distruzione delle registrazioni di comunicazioni o conversazioni intercettate; art. 270-bis c.p.p. che regola le comunicazioni di servizio di appartenenti al Dipartimento delle informazioni per la sicurezza ed ai servizi di informazione per la sicurezza; art. 271 c.p.p. inerente ai divieti di utilizzazione dei risultati ottenuti a seguito di intercettazione (**lett. f**).

Quanto al **sequestro di dati informatici presso fornitori**, la novella all'art. 254-bis c.p.p. prevede che il sequestro è disposto ai sensi dell'articolo 254-ter, comma 12. Si precisa altresì che si applicano le disposizioni di cui al nuovo articolo 254-ter in quanto compatibili (**lett. g**).

Fasi successive al sequestro

Con le modifiche di cui alla **lett. h)** viene estesa ai dispositivi, sistemi informatici o telematici, memorie digitali oggetto di sequestro probatorio la

disciplina contenuta nell'articolo 259 c.p.p. specificamente dettata per la custodia di «dati, informazioni o programmi informatici» sequestrati.

Occorre rammentare che nel caso di custodia per sequestri probatori aventi ad oggetto dati informatici, il custode è tenuto ad impedire l'alterazione dei dati e precludere l'accesso ad essi da parte di terzi, salvo, per quest'ultima ipotesi, apposita autorizzazione dell'autorità giudiziaria. Ciò in considerazione delle peculiarità dei dati informatici e dell'esigenza di evitarne ogni alterazione.

Una modifica puntuale riguarda l'**articolo 293 c.p.p.** che disciplina gli **adempimenti esecutivi dell'ordinanza che dispone la misura cautelare**. Nello specifico si prevede che il difensore, dopo il deposito dell'ordinanza cautelare presso la cancelleria del giudice, abbia il **diritto alla trasposizione** su supporto idoneo, dei dati, informazioni e programmi sottoposti a sequestro ai sensi dell'articolo 254-ter, comma 12, c.p.p. (**lett. i**).

Attraverso la novella di cui alla **lett. o)** viene aggiunto un nuovo comma all'articolo 415-bis c.p.p., il quale disciplina l'istituto dell'**avviso all'indagato della conclusione delle indagini preliminari**.

L'articolo 415-bis c.p.p. regola la *discovery* degli atti di indagine, consentendo all'accusato di prenderne contezza per la prima volta, salvo che nel corso delle indagini preliminari si sia svolto un atto al quale il difensore aveva diritto di assistere (cd. atto garantito). In tal caso, la persona sottoposta alle indagini viene a conoscenza degli addebiti a suo carico attraverso la cd. informazione di garanzia (v. art. 369 c.p.p.).

A norma dell'art. 415-bis, se il pubblico ministero non deve formulare richiesta di archiviazione, fa notificare alla persona sottoposta alle indagini e al difensore, nonché a determinate condizioni anche alla persona offesa, avviso della conclusione delle indagini preliminari (comma 1). Quest'ultimo avviso deve contenere la sommaria enunciazione del fatto per il quale si procede, delle norme di legge che si assumono violate, della data e del luogo del fatto, con l'avvertimento che la documentazione relativa alle indagini espletate è depositata presso la segreteria del pubblico ministero e che l'indagato e il suo difensore hanno facoltà di prenderne visione ed estrarne copia (comma 2).

Ai sensi del **nuovo comma 2-ter** dell'art. 415-bis c.p.p. l'avviso di conclusione delle indagini preliminari deve contenere altresì l'avvertimento che l'indagato e il suo difensore hanno **facoltà di esaminare i dati, le informazioni e i programmi oggetto di sequestro** di cui al comma 12 dell'articolo 254-ter, nonché il diritto alla trasposizione dei dati, delle informazioni o dei programmi medesimi su supporto idoneo.

La disposizione, inoltre, permette al **difensore**, entro il termine di venti giorni, di esaminare il duplicato e di depositare **richiesta motivata di sequestro** dei dati, delle informazioni e dei programmi specificamente indicati come rilevanti in relazione alle circostanze di tempo e di luogo del fatto e alle modalità della condotta, nel rispetto dei criteri di necessità e proporzione. Sull'istanza del difensore provvede il pubblico ministero con decreto motivato. Tuttavia, qualora il pubblico ministero ritenga che non si debba disporre il sequestro, si applica l'articolo 368 c.p.p.

A tal riguardo, si ricorda che l'art. 368 c.p.p. stabilisce che, durante le indagini preliminari, se il pubblico ministero ritiene che non si debba procedere con il sequestro richiesto dall'interessato, trasmette la relativa istanza al giudice per le indagini preliminari, allegando anche il suo parere in merito.

Quando, invece, la richiesta del difensore riguarda dati inerenti a comunicazioni, conversazioni o corrispondenza informatica inviate e ricevute, il pubblico ministero trasmette sempre l'istanza ai sensi dell'articolo 368 e il giudice provvede ai sensi dell'articolo 254-ter, comma 12, secondo e terzo periodo, cp.p..

Si rammenta che il secondo periodo del comma 12 dell'art. 254-ter c.p.p., come introdotto dalla proposta di legge in esame, prescrive che il giudice dispone il sequestro con decreto motivato in presenza dei presupposti di cui agli articoli 266, comma 1, e 267, comma 1 c.p.p.. Mentre il terzo periodo del comma 12 richiama puntualmente la fattispecie dall'art. 13 del D.L. 152 del 1991, il quale regola lo svolgimento di intercettazioni di conversazioni o comunicazioni in relazione “ad un delitto di criminalità organizzata o di minaccia col mezzo del telefono in ordine ai quali sussistano sufficienti indizi”.

Un'ulteriore modifica attiene alla **formazione del fascicolo dibattimentale** di cui all'art. 431 c.p.p. (**lett. p**)

Il comma 1 dell'articolo 431 c.p.p., nella sua formulazione vigente, prevede che immediatamente dopo l'emissione del decreto che dispone il giudizio, il giudice dell'udienza preliminare (G.u.p.) provvede a formare il fascicolo per il dibattimento nel contraddittorio delle parti. Su richiesta di una delle parti la formazione del predetto fascicolo può essere rinviata ad una nuova udienza, da tenersi non oltre il termine di quindici giorni. Per quanto concerne il contenuto del fascicolo, esso comprende: a) gli atti relativi alla procedibilità dell'azione penale e all'esercizio dell'azione civile; b) i verbali degli atti non ripetibili compiuti dalla polizia giudiziaria; c) i verbali degli atti non ripetibili compiuti dal pubblico ministero e dal difensore; d) i documenti acquisiti all'estero mediante rogatoria internazionale e i verbali degli atti non ripetibili assunti con le stesse modalità; e) i verbali degli atti assunti nell'incidente probatorio; f) i verbali degli atti assunti all'estero a seguito di rogatoria internazionale ai quali i difensori sono stati posti in

grado di assistere e di esercitare le facoltà loro consentite dalla legge italiana; g) il certificato generale del casellario giudiziario e gli altri documenti indicati nell'articolo 236, nonché, quando si procede nei confronti di un apolide, di una persona della quale è ignota la cittadinanza, di un cittadino di uno Stato non appartenente all'Unione europea ovvero di un cittadino di uno Stato membro dell'Unione europea privo del codice fiscale o che è attualmente, o è stato in passato, titolare anche della cittadinanza di uno Stato non appartenente all'Unione europea, una copia del cartellino fotodattiloscopico con indicazione del codice univoco identificativo; h) il corpo del reato e le cose pertinenti al reato, qualora non debbano essere custoditi altrove.

Con la novella in commento vengono apportate le seguenti modificazioni all'**art. 431 c.p.p.**:

- al comma 1, lett. *h*) si prevede che debbano essere **ricompresi all'interno del fascicolo per il dibattimento** non solo il corpo del reato e le cose pertinenti al reato, ma anche, in ogni caso, **i supporti di cui all'articolo 254-ter, comma 13** (contenenti i dati, le informazioni e i programmi, debitamente selezionati dal pubblico ministero e sottoposti a sequestro, con le modalità descritte *ex* comma 12 del medesimo articolo). I supporti di cui al periodo precedente sono acquisiti al fascicolo, qualora non debbano essere custoditi altrove;
- viene introdotto il **nuovo comma 1-bis** ai sensi del quale, ai fini della formazione del fascicolo per il dibattimento e ferma la facoltà delle parti di concordare l'acquisizione al fascicolo per il dibattimento di atti contenuti nel fascicolo del pubblico ministero, nonché della documentazione relativa all'attività di investigazione difensiva, il giudice dispone la **trascrizione integrale delle conversazioni o comunicazioni** e la stampa in forma intellegibile delle comunicazioni informatiche o telematiche **oggetto di sequestro ai sensi degli articoli 254-ter, comma 12, e 415-bis, comma 2-ter**, secondo, terzo, quarto e quinto periodo. Si osservano le forme, i modi e le garanzie previste per l'espletamento delle perizie.

L'articolo 2 interviene, poi, sulla disciplina riguardante il **procedimento speciale del giudizio immediato**. In particolare viene modificato l'art. 454 c.p.p. (**lett. q**).

L'articolo 454 c.p.p. disciplina la richiesta di giudizio immediato presentata dal pubblico ministero. Tale richiesta deve essere trasmessa dal pubblico ministero alla cancelleria del giudice per le indagini preliminari entro novanta giorni dalla iscrizione della notizia di reato nell'apposito registro *ex* art. 335 c.p.p. (comma 1). Insieme alla predetta richiesta il pubblico ministero deve trasmettere il fascicolo

contenente la notizia di reato, la documentazione relativa alle indagini espletate e i verbali degli atti compiuti davanti al giudice per le indagini preliminari (comma 2). Peraltro, nel caso in cui non si sia proceduto ai sensi dei commi 4, 5 e 6 dell'articolo 268 c.p.p., con la richiesta di giudizio immediato il pubblico ministero deve depositare anche l'elenco delle intercettazioni di comunicazioni e conversazioni o dei flussi di comunicazioni informatiche o telematiche rilevanti ai fini probatori. La disposizione riconosce inoltre al difensore la facoltà di depositare, entro 15 giorni dalla notifica all'imputato e alla persona offesa della richiesta di giudizio immediato del pubblico ministero (articolo 456, comma 4 c.p.p.), l'elenco delle ulteriori registrazioni ritenute rilevanti e di cui chiede copia. Tale termine può essere prorogato su richiesta del difensore di ulteriori 10 giorni. Sull'istanza provvede il pubblico ministero con decreto motivato. In caso di rigetto dell'istanza o di contestazioni sulle indicazioni relative alle registrazioni ritenute rilevanti il difensore può avanzare al giudice istanza affinché si proceda nelle forme dell'articolo 268, comma 6 (comma 2-*bis*).

La novella di cui alla lett. *q*) aggiunge all'art. 454 c.p.p. il **nuovo comma 2-ter**, il quale sancisce che entro il medesimo termine di cui al comma 2-*bis*, secondo periodo, (e quindi entro quindici giorni dalla notifica) il difensore può esaminare il duplicato informatico conservato ai sensi dell'articolo 254-*ter*, comma 16, ai fini dell'eventuale richiesta di cui all'articolo 415-*bis*, comma 2-*ter*, secondo periodo (vedi art. 2 lett. *o*) della proposta di legge in esame), da formulare in sede di richieste di giudizio abbreviato di cui all'art. 438, comma 5, ovvero di ammissione di prove di cui all'art. 493 c.p.p..

Infine, viene novellata la disciplina dettata in tema di **opposizione al decreto penale** di cui all'art. 461 c.p.p. (**lett. *r***).

In particolare, l'art. 461 c.p.p. stabilisce che l'imputato e la persona civilmente obbligata per la pena pecuniaria, personalmente o a mezzo del difensore eventualmente nominato, possono proporre opposizione nella cancelleria del giudice per le indagini preliminari che ha emesso il decreto ovvero nella cancelleria del tribunale o del giudice di pace del luogo in cui si trova l'opponente, nel termine di quindici giorni e con le forme previste dall'articolo 582 (comma 1)

Il **nuovo comma 1-*bis*** dell'art. 461 c.p.p. prescrive che entro quindici giorni dalla notificazione del decreto, il difensore può esaminare il duplicato informatico conservato ai sensi dell'articolo 254-*ter*, comma 16, ai fini dell'eventuale richiesta di cui all'articolo 415-*bis*, comma 2-*ter*, secondo periodo (vedi art. 2 lett. *o*) della proposta di legge in esame), da formulare in sede di richieste di giudizio abbreviato di cui all'articolo 438, comma 5, ovvero di ammissione di prove di cui all'articolo 493 c.p.p.

Articolo 3

(Modifica alle norme di attuazione, di coordinamento e transitorie del codice di procedura penale)

L'**articolo 3** introduce nelle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, due nuove disposizioni: **l'articolo 82-bis** in materia di **attività per la custodia dei supporti contenenti dati, informazioni e programmi sottoposti a sequestro** e **l'articolo 82-ter** che disciplina **la conservazione dei duplicati informatici**.

Più nel dettaglio **l'articolo 82-bis** prevede che i supporti sui quali sono riversati i dati, le informazioni e i programmi sottoposti a sequestro informatico devono essere racchiusi in apposite custodie numerate. Ogni custodia, a sua volta, deve essere racchiusa in un involucro, sul quale sono indicati gli estremi del procedimento e del provvedimento di sequestro. Ove necessario per garantirne la protezione, i supporti possono essere conservati anche in contenitori separati dagli atti processuali. Nel caso in cui tali modalità di conservazione non siano possibili debbono essere comunque adottate modalità idonee a garantire la protezione dei supporti.

L'**articolo 82-ter** invece, prevede che al fine di garantire che la conservazione dei supporti contenenti il duplicato informatico assicuri l'assoluta riservatezza si applicano le disposizioni di cui all'articolo 89-bis, comma 2, secondo periodo, (ai sensi del quale il Procuratore della Repubblica impartisce, con particolare riguardo alle modalità di accesso all'archivio delle intercettazioni, le prescrizioni necessarie a garantire la tutela del segreto su quanto ivi custodito) e comma 3 (che prevede che all'archivio possono accedere il giudice che procede e i suoi ausiliari, il pubblico ministero e i suoi ausiliari, ivi compresi gli ufficiali di polizia giudiziaria delegati all'ascolto, i difensori delle parti, assistiti, se necessario, da un interprete. Ogni accesso è annotato in apposito registro, gestito con modalità informatiche; in esso sono indicate data, ora iniziale e finale, e gli atti specificamente consultati). L'accesso ai supporti è consentito, con le medesime cautele e prescrizioni, anche ai consulenti tecnici nominati.

Articolo 4
(Disposizione transitoria)

L'articolo 4 reca infine una **disposizione transitoria** relativa alla decorrenza di applicazione della nuova disciplina.

Ai sensi dell'**articolo 4** le disposizioni di cui alla proposta di legge in esame si applicano alle perquisizioni e ai sequestri la cui esecuzione ha avuto inizio in data successiva a quella della sua entrata in vigore.

Testo a fronte

Codice di procedura penale	
Testo vigente	Testo come modificato dall'A.C. 1822
Art. 114 (Divieto di pubblicazione di atti e di immagini)	Art. 114 (idem)
	[articolo 2, comma 1, lett. a)]
1. È vietata la pubblicazione, anche parziale o per riassunto, con il mezzo della stampa o con altro mezzo di diffusione, degli atti coperti dal segreto o anche solo del loro contenuto.	Identico.
2. È vietata la pubblicazione, anche parziale, degli atti non più coperti dal segreto fino a che non siano concluse le indagini preliminari ovvero fino al termine dell'udienza preliminare, fatta eccezione per l'ordinanza indicata dall'articolo 292.	Identico.
2-bis. È sempre vietata la pubblicazione, anche parziale, del contenuto delle intercettazioni se non è riprodotto dal giudice nella motivazione di un provvedimento o utilizzato nel corso del dibattimento.	2-bis. È sempre vietata la pubblicazione, anche parziale, del contenuto delle intercettazioni se non è riprodotto dal giudice nella motivazione di un provvedimento o utilizzato nel corso del dibattimento, nonché del contenuto dei duplicati formati ai sensi dell'articolo 254-ter, diversi dai dati, dalle informazioni e dai programmi sequestrati ai sensi del comma 12 del medesimo articolo 254-ter [novella irriferribile ndr].
3. Se si procede al dibattimento, non è consentita la pubblicazione, anche parziale, degli atti del fascicolo per il dibattimento, se non dopo la pronuncia della sentenza di primo grado, e di quelli del fascicolo del pubblico ministero, se non dopo la pronuncia della sentenza in grado di appello. È sempre consentita la pubblicazione degli atti utilizzati per le contestazioni.	Identico.
4. È vietata la pubblicazione, anche parziale, degli atti del dibattimento celebrato a porte chiuse nei casi previsti dall'articolo 472 commi 1 e 2. In tali casi il giudice, sentite le parti, può disporre il	Identico.

Codice di procedura penale	
Testo vigente	Testo come modificato dall'A.C. 1822
divieto di pubblicazione anche degli atti o di parte degli atti utilizzati per le contestazioni. Il divieto di pubblicazione cessa comunque quando sono trascorsi i termini stabiliti dalla legge sugli archivi di Stato ovvero è trascorso il termine di dieci anni dalla sentenza irrevocabile e la pubblicazione è autorizzata dal ministro di grazia e giustizia.	
5. Se non si procede al dibattimento, il giudice, sentite le parti, può disporre il divieto di pubblicazione di atti o di parte di atti quando la pubblicazione di essi può offendere il buon costume o comportare la diffusione di notizie sulle quali la legge prescrive di mantenere il segreto nell'interesse dello Stato ovvero causare pregiudizio alla riservatezza dei testimoni o delle parti private. Si applica la disposizione dell'ultimo periodo del comma 4.	<i>Identico.</i>
6. È vietata la pubblicazione delle generalità e dell'immagine dei minorenni testimoni, persone offese o danneggiati dal reato fino a quando non sono divenuti maggiorenni. È altresì vietata la pubblicazione di elementi che anche indirettamente possano comunque portare alla identificazione dei suddetti minorenni. Il tribunale per i minorenni, nell'interesse esclusivo del minorenne, o il minorenne che ha compiuto i sedici anni, può consentire la pubblicazione.	<i>Identico.</i>
6-bis. È vietata la pubblicazione dell'immagine di persona privata della libertà personale ripresa mentre la stessa si trova sottoposta all'uso di manette ai polsi ovvero ad altro mezzo di coercizione fisica, salvo che la persona vi consenta.	<i>Identico.</i>
7. È sempre consentita la pubblicazione del contenuto di atti non coperti dal segreto.	<i>Identico.</i>
Art. 233 (Consulenza tecnica fuori dei casi di	Art. 233 (idem)

Codice di procedura penale	
Testo vigente	Testo come modificato dall'A.C. 1822
<i>perizia)</i>	
	[articolo 2, comma 1, lett. b)]
1. Quando non è stata disposta perizia, ciascuna parte può nominare, in numero non superiore a due, propri consulenti tecnici. Questi possono esporre al giudice il proprio parere, anche presentando memorie a norma dell'articolo 121.	Identico.
1-bis. Il giudice, a richiesta del difensore, può autorizzare il consulente tecnico di una parte privata ad esaminare le cose sequestrate nel luogo in cui esse si trovano, ad intervenire alle ispezioni, ovvero ad esaminare l'oggetto delle ispezioni alle quali il consulente non è intervenuto. Prima dell'esercizio dell'azione penale l'autorizzazione è disposta dal pubblico ministero a richiesta del difensore. Contro il decreto che respinge la richiesta il difensore può proporre opposizione al giudice, che provvede nelle forme di cui all'articolo 127.	Identico.
1-ter. L'autorità giudiziaria impartisce le prescrizioni necessarie per la conservazione dello stato originario delle cose e dei luoghi e per il rispetto delle persone.	Identico.
	1-quater. Il consulente tecnico ha facoltà di assistere, senza preavviso, alla perquisizione di un sistema informatico o telematico, di un dispositivo o di una memoria digitale, disposta ai sensi dell'articolo 247, comma 1-bis, o eseguita ai sensi dell'articolo 352, comma 1-bis, e può formulare osservazioni e riserve.
2. Qualora, successivamente alla nomina del consulente tecnico, sia disposta perizia, ai consulenti tecnici già nominati sono riconosciuti i diritti e le facoltà previsti dall'articolo 230, salvo il limite previsto dall'articolo 225 comma 1.	Identico.
3. Si applica la disposizione dell'articolo 225 comma 3.	Identico.
Art. 247 (Casi e forme delle perquisizioni)	Art. 247 (idem)

Codice di procedura penale	
Testo vigente	Testo come modificato dall'A.C. 1822
	[articolo 2, comma 1, lett. c)]
1. Quando vi è fondato motivo di ritenere che taluno occulti sulla persona il corpo del reato o cose pertinenti al reato, è disposta perquisizione personale. Quando vi è fondato motivo di ritenere che tali cose si trovino in un determinato luogo ovvero che in esso possa eseguirsi l'arresto dell'imputato o dell'evaso, è disposta perquisizione locale.	<i>Identico.</i>
1-bis. Quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorché protetto da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione.	1-bis. Quando vi è fondato motivo di ritenere che determinati dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, in un dispositivo o in una memoria digitale , ancorché protetti da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione.
2. La perquisizione è disposta con decreto motivato.	<i>Identico.</i>
3. L'autorità giudiziaria può procedere personalmente ovvero disporre che l'atto sia compiuto da ufficiali di polizia giudiziaria delegati con lo stesso decreto.	<i>Identico.</i>
	Art. 250-bis (Perquisizioni di dispositivi, sistemi informatici o telematici o memorie digitali)
	[articolo 2, comma 1, lett. d)]
	1. Quando la perquisizione è disposta ai sensi dell'articolo 247, comma 1-bis, nell'atto di iniziare le operazioni, copia del decreto di perquisizione è consegnata all'imputato, se presente, e a chi abbia l'attuale disponibilità del sistema informatico o telematico, del dispositivo o della memoria digitale, con l'avviso della facoltà di farsi rappresentare o assistere da persona di fiducia, purché questa sia prontamente reperibile e idonea a norma dell'articolo 120. L'imputato presente è,

Codice di procedura penale	
Testo vigente	Testo come modificato dall'A.C. 1822
	altresì, avvisato della facoltà di farsi assistere da un consulente tecnico, purché questo sia prontamente reperibile.
	2. Se mancano le persone indicate nel comma 1, la copia è consegnata e l'avviso della facoltà di cui al comma 1, primo periodo, è rivolto a un congiunto, un coabitante o un collaboratore.
Art. 252 (Sequestro conseguente a perquisizione)	Art. 252 (idem)
	[articolo 2, comma 1, lett. e)]
1. Le cose rinvenute a seguito della perquisizione sono sottoposte a sequestro con l'osservanza delle prescrizioni degli articoli 259 e 260.	Identico.
	1-bis. I dati, le informazioni o i programmi rinvenuti a seguito della perquisizione eseguita ai sensi dell'articolo 247, comma 1-bis, sono sottoposti a sequestro nel rispetto dei presupposti di cui all'articolo 254-ter, comma 12. L'acquisizione dei dati, delle informazioni o dei programmi sottoposti a sequestro è in ogni caso effettuata ai sensi dell'articolo 254-ter, comma 13. Se i dati sono inerenti a comunicazioni, conversazioni e corrispondenza informatica inviate e ricevute, il pubblico ministero richiede al giudice la convalida e l'emissione del decreto di sequestro entro quarantotto ore dall'esecuzione.
	1-ter. Quando, a seguito della perquisizione eseguita ai sensi dell'articolo 247, comma 1-bis, risulta necessario sottoporre a sequestro il dispositivo o il sistema informatico o telematico o la memoria digitale oggetto della perquisizione, si applicano le disposizioni di cui all'articolo 254-ter e il pubblico ministero procede ai sensi del comma 4 dello stesso articolo.
Art. 254 (Sequestro di corrispondenza)	Art. 254 (idem)

Codice di procedura penale	
Testo vigente	Testo come modificato dall'A.C. 1822
	[articolo 2, comma 1, lett. f)]
1. Presso coloro che forniscono servizi postali, telegrafici, telematici o di telecomunicazioni è consentito procedere al sequestro di lettere, pieghi, pacchi, valori, telegrammi e altri oggetti di corrispondenza, anche se inoltrati per via telematica, che l'autorità giudiziaria abbia fondato motivo di ritenere spediti dall'imputato o a lui diretti, anche sotto nome diverso o per mezzo di persona diversa, o che comunque possono avere relazione con il reato.	Identico.
	1-bis. Il sequestro è disposto dal giudice in presenza dei presupposti di cui all'articolo 254-ter, comma 12, fermo, per i casi di urgenza, il disposto del comma 4 del medesimo articolo. Si applica il comma 14 dell'articolo 254-ter.
2. Quando al sequestro procede un ufficiale di polizia giudiziaria, questi deve consegnare all'autorità giudiziaria gli oggetti di corrispondenza sequestrati, senza aprirli o alterarli e senza prendere altrimenti conoscenza del loro contenuto.	Identico.
3. Le carte e gli altri documenti sequestrati che non rientrano fra la corrispondenza sequestrabile sono immediatamente restituiti all'avente diritto e non possono comunque essere utilizzati.	Identico.
Art. 254-bis (Sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni)	Art. 254-bis (idem)
	[articolo 2, comma 1, lett. g)]
1. L'autorità giudiziaria, quando dispone il sequestro, presso i fornitori di servizi informatici, telematici o di telecomunicazioni, dei dati da questi detenuti, compresi quelli di traffico o di ubicazione, può stabilire, per esigenze legate alla regolare fornitura dei medesimi servizi, che la loro acquisizione avvenga	Identico.

Codice di procedura penale	
Testo vigente	Testo come modificato dall'A.C. 1822
mediante copia di essi su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità. In questo caso è, comunque, ordinato al fornitore dei servizi di conservare e proteggere adeguatamente i dati originali.	
	1-bis. Il sequestro è disposto ai sensi dell'articolo 254-ter, comma 12.
	1-ter. Si applicano le disposizioni dell'articolo 254-ter in quanto compatibili.
	Art. 254-ter <i>(Sequestro di dispositivi e sistemi informatici o telematici, memorie digitali, dati, informazioni, programmi, comunicazioni e corrispondenza informatica inviate e ricevute)</i>
	<i>[articolo 1, comma 1]</i>
	1. Nel corso delle indagini preliminari, il giudice per le indagini preliminari, a richiesta del pubblico ministero, dispone con decreto motivato il sequestro di dispositivi e sistemi informatici o telematici o di memorie digitali, necessari per la prosecuzione delle indagini in relazione alle circostanze di tempo e di luogo del fatto e alle modalità della condotta, nel rispetto del criterio di proporzione. Il decreto che dispone il sequestro è immediatamente trasmesso, a cura della cancelleria, al pubblico ministero, che ne cura l'esecuzione.
	2. Il pubblico ministero può procedere all'esecuzione personalmente ovvero disporre che l'atto sia compiuto da ufficiali di polizia giudiziaria. Il sequestro è eseguito con modalità tecniche idonee ad evitare l'alterazione o la perdita dei dati e, a tal fine, il pubblico ministero adotta le misure tecniche necessarie o impartisce specifiche

Codice di procedura penale	
Testo vigente	Testo come modificato dall'A.C. 1822
	prescrizioni. Copia del decreto di sequestro è consegnata all'interessato, se presente.
	3. Il sequestro è immediatamente revocato dal pubblico ministero con decreto motivato, quando risultano mancanti, anche per fatti sopravvenuti, le condizioni di applicabilità previste dal comma 1. Il decreto è notificato a coloro che hanno diritto di proporre impugnazione. Se vi è richiesta di revoca dell'interessato, il pubblico ministero, quando ritiene che essa vada anche soltanto in parte respinta, la trasmette al giudice, cui presenta richieste specifiche nonché gli elementi sui quali fonda le sue valutazioni. La richiesta di revoca è trasmessa non oltre il giorno successivo a quello del deposito nella segreteria.
	4. Quando non è possibile, per la situazione di urgenza, attendere il provvedimento del giudice, il sequestro è disposto con decreto motivato dal pubblico ministero. Negli stessi casi, prima dell'intervento del pubblico ministero, al sequestro procedono ufficiali di polizia giudiziaria, i quali, nelle quarantotto ore successive, trasmettono il verbale al pubblico ministero del luogo in cui il sequestro è stato eseguito. Questi, se non dispone la restituzione delle cose sequestrate, richiede al giudice la convalida e l'emissione del decreto previsto dal comma 1 entro quarantotto ore dal sequestro, se disposto dallo stesso pubblico ministero, o dalla ricezione del verbale, se il sequestro è stato eseguito di

Codice di procedura penale	
Testo vigente	Testo come modificato dall'A.C. 1822
	iniziativa dalla polizia giudiziaria.
	5. Il sequestro perde efficacia se non sono osservati i termini previsti dal comma 4 ovvero se il giudice non emette l'ordinanza di convalida entro dieci giorni dalla ricezione della richiesta. Copia dell'ordinanza è immediatamente notificata alla persona alla quale le cose sono state sequestrate.
	6. Entro cinque giorni dal deposito del verbale di sequestro, il pubblico ministero avvisa la persona sottoposta alle indagini, la persona alla quale le cose sono state sequestrate e quella che avrebbe diritto alla loro restituzione, la persona offesa dal reato e i relativi difensori del giorno, dell'ora e del luogo fissati per il conferimento dell'incarico per la duplicazione del contenuto dei dispositivi informatici, dei sistemi informatici o telematici o delle memorie digitali in sequestro, e della facoltà di nominare consulenti tecnici. Il pubblico ministero può disporre che sia effettuata la duplicazione anche dei dati, delle informazioni o dei programmi accessibili da remoto dal dispositivo in sequestro. Tra l'avviso e la data fissata per il conferimento dell'incarico non può intercorrere un termine superiore a dieci giorni. Si applicano le disposizioni dell'articolo 364, comma 2.
	7. Il pubblico ministero può autorizzare la persona sottoposta alle indagini, la persona offesa dal reato, la persona alla quale le cose sono state sequestrate e quella che avrebbe diritto alla loro restituzione, i difensori e i consulenti

Codice di procedura penale	
Testo vigente	Testo come modificato dall'A.C. 1822
	tecnici eventualmente nominati, che ne facciano richiesta, a partecipare a distanza al conferimento dell'incarico.
	8. Fermo il diritto dei soggetti indicati al comma 6 di assistere al conferimento dell'incarico, i difensori nonché i consulenti tecnici eventualmente nominati hanno diritto altresì di partecipare allo svolgimento delle operazioni di duplicazione e di formulare osservazioni e riserve.
	9. La duplicazione avviene su adeguati supporti informatici mediante una procedura che assicuri la conformità del duplicato all'originale e la sua immodificabilità.
	10. Nei procedimenti di cui agli articoli 406, comma 5-bis, e 371-bis, comma 4-bis, nonché quando sussiste un pericolo per la vita o l'incolumità di una persona o la sicurezza dello Stato, ovvero un pericolo di concreto pregiudizio per le indagini in corso, o un pericolo attuale di cancellazione o dispersione dei dati, delle informazioni o dei programmi, la duplicazione può avvenire in deroga al disposto dei commi 6, 7 e 8, con modalità tecniche idonee ad assicurare la conformità del duplicato all'originale e la sua immodificabilità.
	11. Fermo quanto stabilito dal comma 3, il pubblico ministero, effettuata la duplicazione, dispone senza ritardo la restituzione dei dispositivi informatici, dei sistemi informatici o telematici o delle memorie digitali all'avente diritto. Non si fa luogo alla restituzione e il sequestro è mantenuto ai fini preventivi

Codice di procedura penale	
Testo vigente	Testo come modificato dall'A.C. 1822
	quando il giudice provvede a norma dell'articolo 321.
	12. Effettuata l'analisi del duplicato informatico, il pubblico ministero procede con decreto motivato al sequestro dei dati, delle informazioni e dei programmi strettamente pertinenti al reato in relazione alle circostanze di tempo e di luogo del fatto e alle modalità della condotta, nel rispetto dei criteri di necessità e proporzione. Qualora il pubblico ministero intenda procedere al sequestro dei dati inerenti a comunicazioni, conversazioni o corrispondenza informatica inviate e ricevute, lo richiede al giudice per le indagini preliminari, che provvede con decreto motivato, disponendo il sequestro in presenza dei presupposti di cui al primo periodo e agli articoli 266, comma 1, e 267, comma 1. Nei procedimenti rispetto ai quali trova applicazione l'articolo 13 del decreto-legge 13 maggio 1991, n. 152, convertito, con modificazioni, dalla legge 12 luglio 1991, n. 203, il giudice dispone il sequestro in presenza dei presupposti indicati nel medesimo articolo 13. Copia del decreto di sequestro è notificata all'avente diritto alla restituzione del dispositivo.
	13. I dati, le informazioni e i programmi sottoposti a sequestro ai sensi del comma 12 sono riversati su idonei supporti con modalità tecniche idonee ad assicurare la loro conformità ai medesimi dati, informazioni e programmi contenuti nel duplicato e la loro immutabilità. I supporti di cui al periodo precedente

Codice di procedura penale	
Testo vigente	Testo come modificato dall'A.C. 1822
	sono acquisiti al fascicolo.
	14. Si applicano, in quanto compatibili, le disposizioni di cui agli articoli 103, 269, commi 2 e 3, 270, commi 1, 2 e 3, 270-bis e 271.
	15. Salvi i casi di cui all'articolo 419, comma 3, dopo l'esercizio dell'azione penale il sequestro ai sensi dei commi 1 e 12 del presente articolo è disposto dal giudice che procede. In tal caso, alla duplicazione si procede con perizia.
	16. La conservazione del duplicato informatico avviene presso la procura della Repubblica, in luogo protetto da specifiche misure di sicurezza, con modalità tali da assicurare l'assoluta riservatezza.
	17. Il duplicato informatico è conservato fino alla sentenza o al decreto penale di condanna non più soggetti a impugnazione. Tuttavia gli interessati, quando i dati, le informazioni e i programmi contenuti nel duplicato non sono necessari per il procedimento, possono chiederne la distruzione, a tutela della riservatezza, al giudice che ha disposto o convalidato il sequestro di cui al comma 1. Il giudice decide in camera di consiglio a norma dell'articolo 127. In caso di archiviazione, il giudice dispone l'immediata distruzione del duplicato informatico, salvo che, anche su istanza di uno dei soggetti indicati dall'articolo 409, comma 2, ritenga sussistenti specifiche esigenze che ne impongono la conservazione.
	18. La distruzione, nei casi in cui è prevista, è eseguita sotto controllo del giudice. Dell'operato è redatto verbale.

Codice di procedura penale	
Testo vigente	Testo come modificato dall'A.C. 1822
	19. Contro i provvedimenti emessi ai sensi dei commi 1, 4 e 12 del presente articolo è ammesso riesame ai sensi dell'articolo 257.
Art. 259 (Custodia delle cose sequestrate)	Art. 259 (idem)
	[articolo 2, comma 1, lett. h)]
1. Le cose sequestrate sono affidate in custodia alla cancelleria o alla segreteria. Quando ciò non è possibile o non è opportuno, l'autorità giudiziaria dispone che la custodia avvenga in luogo diverso, determinandone il modo e nominando un altro custode, idoneo a norma dell'articolo 120.	Identico.
2. All'atto della consegna, il custode è avvertito dell'obbligo di conservare e di presentare le cose a ogni richiesta dell'autorità giudiziaria nonché delle pene previste dalla legge penale per chi trasgredisce ai doveri della custodia. Quando la custodia riguarda dati, informazioni o programmi informatici, il custode è altresì avvertito dell'obbligo di impedirne l'alterazione o l'accesso da parte di terzi, salva, in quest'ultimo caso, diversa disposizione dell'autorità giudiziaria. Al custode può essere imposta una cauzione. Dell'avvenuta consegna, dell'avvertimento dato e della cauzione imposta è fatta menzione nel verbale. La cauzione è ricevuta, con separato verbale, nella cancelleria o nella segreteria.	2. All'atto della consegna, il custode è avvertito dell'obbligo di conservare e di presentare le cose a ogni richiesta dell'autorità giudiziaria nonché delle pene previste dalla legge penale per chi trasgredisce ai doveri della custodia. Quando la custodia riguarda dispositivi, sistemi informatici o telematici, memorie digitali ovvero dati, informazioni o programmi informatici, il custode è altresì avvertito dell'obbligo di impedirne l'alterazione o l'accesso da parte di terzi, salva, in quest'ultimo caso, diversa disposizione dell'autorità giudiziaria. Al custode può essere imposta una cauzione. Dell'avvenuta consegna, dell'avvertimento dato e della cauzione imposta è fatta menzione nel verbale. La cauzione è ricevuta, con separato verbale, nella cancelleria o nella segreteria.
Art. 293 (Adempimenti esecutivi)	Art. 293 (idem)
	[articolo 2, comma 1, lett. i)]
1. Salvo quanto previsto dall'articolo 156, l'ufficiale o l'agente incaricato di eseguire l'ordinanza che ha disposto la custodia cautelare consegna all'imputato copia del provvedimento unitamente a una	Identico.

Codice di procedura penale	
Testo vigente	Testo come modificato dall'A.C. 1822
comunicazione scritta, redatta in forma chiara e precisa e, per l'imputato che non conosce la lingua italiana, tradotta in una lingua a lui comprensibile, con cui lo informa: a) della facoltà di nominare un difensore di fiducia e di essere ammesso al patrocinio a spese dello Stato nei casi previsti dalla legge; b) del diritto di ottenere informazioni in merito all'accusa; c) del diritto all'interprete ed alla traduzione di atti fondamentali; d) del diritto di avvalersi della facoltà di non rispondere; e) del diritto di accedere agli atti sui quali si fonda il provvedimento; f) del diritto di informare le autorità consolari e di dare avviso ai familiari; g) del diritto di accedere all'assistenza medica di urgenza; h) del diritto di essere condotto davanti all'autorità giudiziaria non oltre cinque giorni dall'inizio dell'esecuzione, se la misura applicata è quella della custodia cautelare in carcere ovvero non oltre dieci giorni se la persona è sottoposta ad altra misura cautelare; i) del diritto di comparire dinanzi al giudice per rendere l'interrogatorio, di impugnare l'ordinanza che dispone la misura cautelare e di richiederne la sostituzione o la revoca; i-bis) della facoltà di accedere ai programmi di giustizia riparativa.	
1-bis. Qualora la comunicazione scritta di cui al comma 1 non sia prontamente disponibile in una lingua comprensibile all'imputato, le informazioni sono fornite oralmente, salvo l'obbligo di dare comunque, senza ritardo, comunicazione scritta all'imputato.	<i>Identico.</i>
1-ter. L'ufficiale o l'agente incaricato di	<i>Identico.</i>

Codice di procedura penale	
Testo vigente	Testo come modificato dall'A.C. 1822
e eseguire l'ordinanza informa immediatamente il difensore di fiducia eventualmente nominato ovvero quello di ufficio designato a norma dell'articolo 97 e redige verbale di tutte le operazioni compiute, facendo menzione della consegna della comunicazione di cui al comma 1 o dell'informazione orale fornita ai sensi del comma 1-bis. Il verbale è immediatamente trasmesso al giudice che ha emesso l'ordinanza e al pubblico ministero.	
2. Le ordinanze che dispongono misure diverse dalla custodia cautelare sono notificate all'imputato.	<i>Identico.</i>
3. Le ordinanze previste dai commi 1 e 2, dopo la loro notificazione o esecuzione, sono depositate nella cancelleria del giudice che le ha emesse insieme alla richiesta del pubblico ministero e agli atti presentati con la stessa. Avviso del deposito è notificato al difensore. Il difensore ha diritto di esaminare e di estrarre copia dei verbali delle comunicazioni e conversazioni intercettate di cui all'articolo 291, comma 1. Ha in ogni caso diritto alla trasposizione, su supporto idoneo alla riproduzione dei dati, delle relative registrazioni.	3. Le ordinanze previste dai commi 1 e 2, dopo la loro notificazione o esecuzione, sono depositate nella cancelleria del giudice che le ha emesse insieme alla richiesta del pubblico ministero e agli atti presentati con la stessa. Avviso del deposito è notificato al difensore. Il difensore ha diritto di esaminare e di estrarre copia dei verbali delle comunicazioni e conversazioni intercettate di cui all'articolo 291, comma 1. Ha in ogni caso diritto alla trasposizione, su supporto idoneo alla riproduzione dei dati, delle relative registrazioni. Il difensore ha altresì diritto alla trasposizione, su supporto idoneo, dei dati, delle informazioni e dei programmi sequestrati ai sensi del comma 12 dell'articolo 254-ter.
Art. 352 (Perquisizioni)	Art. 352 (idem)
	[articolo 2, comma 1, lett. l)]
1. Nella flagranza del reato o nel caso di evasione, gli ufficiali di polizia giudiziaria procedono a perquisizione personale o locale quando hanno fondato motivo di ritenere che sulla persona si trovino	<i>Identico.</i>

Codice di procedura penale	
Testo vigente	Testo come modificato dall'A.C. 1822
occultate cose o tracce pertinenti al reato che possono essere cancellate o disperse ovvero che tali cose o tracce si trovino in un determinato luogo o che ivi si trovi la persona sottoposta alle indagini o l'evaso.	
1-bis. Nella flagranza del reato, ovvero nei casi di cui al comma 2 quando sussistono i presupposti e le altre condizioni ivi previsti, gli ufficiali di polizia giudiziaria, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione, procedono altresì alla perquisizione di sistemi informatici o telematici, ancorché protetti da misure di sicurezza, quando hanno fondato motivo di ritenere che in questi si trovino occultati dati, informazioni, programmi informatici o tracce comunque pertinenti al reato che possono essere cancellati o dispersi.	1-bis. Nella flagranza del reato, ovvero nei casi di cui al comma 2 quando sussistono i presupposti e le altre condizioni ivi previsti, gli ufficiali di polizia giudiziaria, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione, procedono altresì alla perquisizione di dispositivi , sistemi informatici o telematici o memorie digitali , ancorché protetti da misure di sicurezza, quando hanno fondato motivo di ritenere che in questi si trovino occultati dati, informazioni, programmi informatici o tracce comunque pertinenti al reato che possono essere cancellati o dispersi. In tal caso, la polizia giudiziaria avvisa l'indagato presente della facoltà di farsi assistere da un consulente tecnico, purché questo sia prontamente reperibile.
	1-ter. I dati, le informazioni o i programmi rinvenuti a seguito della perquisizione di cui al comma 1-bis sono sottoposti a sequestro nel rispetto dei presupposti di cui all'articolo 254-ter, comma 12. L'acquisizione dei dati, delle informazioni o dei programmi sottoposti a sequestro è in ogni caso effettuata ai sensi dell'articolo 254-ter, comma 13.
2. Quando si deve procedere alla esecuzione di un'ordinanza che dispone la custodia cautelare o di un ordine che dispone la carcerazione nei confronti di persona imputata o condannata per uno dei delitti previsti dall'articolo 380 ovvero al fermo di una persona indiziata di delitto, gli ufficiali di polizia giudiziaria possono altresì procedere a perquisizione personale o locale se ricorrono i presupposti indicati nel comma 1 e sussistono particolari motivi	<i>Identico.</i>

Codice di procedura penale	
Testo vigente	Testo come modificato dall'A.C. 1822
di urgenza che non consentono la emissione di un tempestivo decreto di perquisizione.	
3. La perquisizione domiciliare può essere eseguita anche fuori dei limiti temporali dell'articolo 251 quando il ritardo potrebbe pregiudicarne l'esito.	<i>Identico.</i>
4. La polizia giudiziaria trasmette senza ritardo, e comunque non oltre le quarantotto ore, al pubblico ministero del luogo dove la perquisizione è stata eseguita il verbale delle operazioni compiute. Il pubblico ministero, nelle quarantotto ore successive, decide con decreto motivato sulla convalida della perquisizione.	<i>Identico.</i>
4-bis. Salvo che alla perquisizione sia seguito il sequestro, entro dieci giorni dalla data in cui hanno avuto conoscenza del decreto di convalida, la persona nei cui confronti vengono svolte le indagini e la persona nei cui confronti la perquisizione è stata disposta o eseguita possono proporre opposizione, sulla quale il giudice provvede a norma dell'articolo 127. Si applica la disposizione di cui all'articolo 252-bis, comma 3.	<i>Identico.</i>
Art. 354 (Accertamenti urgenti sui luoghi, sulle cose e sulle persone. Sequestro)	Art. 354 (idem)
	[articolo 2, comma 1, lett. m)]
1. Gli ufficiali e gli agenti di polizia giudiziaria curano che le tracce e le cose pertinenti al reato siano conservate e che lo stato dei luoghi e delle cose non venga mutato prima dell'intervento del pubblico ministero.	<i>Identico.</i>
2. Se vi è pericolo che le cose, le tracce e i luoghi indicati nel comma 1 si alterino o si disperdano o comunque si modifichino e il pubblico ministero non può intervenire tempestivamente, ovvero non ha ancora assunto la direzione delle indagini, gli ufficiali di polizia giudiziaria compiono i necessari accertamenti e rilievi sullo stato dei luoghi e delle cose. In relazione ai dati,	2. Se vi è pericolo che le cose, le tracce e i luoghi indicati nel comma 1 si alterino o si disperdano o comunque si modifichino e il pubblico ministero non può intervenire tempestivamente, ovvero non ha ancora assunto la direzione delle indagini, gli ufficiali di polizia giudiziaria compiono i necessari accertamenti e rilievi sullo stato dei luoghi e delle cose. In relazione ai

Codice di procedura penale	
Testo vigente	Testo come modificato dall'A.C. 1822
alle informazioni e ai programmi informatici o ai sistemi informatici o telematici , gli ufficiali della polizia giudiziaria adottano, altresì, le misure tecniche o impartiscono le prescrizioni necessarie ad assicurarne la conservazione e ad impedirne l'alterazione e l'accesso e provvedono, ove possibile, alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immutabilità. Se del caso, sequestrano il corpo del reato e le cose a questo pertinenti.	dispositivi, ai sistemi informatici o telematici o alle memorie digitali ovvero ai dati, alle informazioni e ai programmi informatici, gli ufficiali della polizia giudiziaria adottano altresì le misure tecniche o impartiscono le prescrizioni necessarie ad assicurarne la conservazione e a impedirne l'alterazione e l'accesso. Se del caso, sequestrano il corpo del reato e le cose a questo pertinenti, osservando le disposizioni di cui all'articolo 352, comma 1-ter, quando il sequestro ha ad oggetto dati, informazioni o programmi informatici.
	2-bis. Quando risulta necessario sottoporre a sequestro un dispositivo, un sistema informatico o telematico o una memoria digitale, si applicano le disposizioni di cui all'articolo 254-ter e la polizia giudiziaria procede ai sensi del comma 4 dello stesso articolo.
3. Se ricorrono i presupposti previsti dal comma 2, gli ufficiali di polizia giudiziaria compiono i necessari accertamenti e rilievi sulle persone diversi dalla ispezione personale.	<i>Identico.</i>
Art. 355 (<i>Convalida del sequestro e suo riesame</i>)	Art. 355 (<i>idem</i>)
	[articolo 2, comma 1, lett. n)]
1. Nel caso in cui abbia proceduto a sequestro, la polizia giudiziaria enuncia nel relativo verbale il motivo del provvedimento e ne consegna copia alla persona alla quale le cose sono state sequestrate. Il verbale è trasmesso senza ritardo, e comunque non oltre le quarantotto ore, al pubblico ministero del luogo dove il sequestro è stato eseguito.	<i>Identico.</i>
2. Il pubblico ministero, nelle quarantotto ore successive, con decreto motivato convalida il sequestro se ne ricorrono i presupposti ovvero dispone la restituzione delle cose sequestrate. Copia del decreto di convalida è immediatamente notificata alla	<i>Identico.</i>

Codice di procedura penale	
Testo vigente	Testo come modificato dall'A.C. 1822
persona alla quale le cose sono state sequestrate.	
	2-bis. Quando il sequestro di cui agli articoli 352, comma 1-ter, e 354, comma 2-bis, ha ad oggetto dati inerenti a comunicazioni, conversazioni e corrispondenza informatica inviate e ricevute, il pubblico ministero richiede al giudice la convalida e l'emissione del decreto di sequestro entro quarantotto ore dall'esecuzione.
3. Contro il decreto di convalida, la persona nei cui confronti vengono svolte le indagini e il suo difensore, la persona alla quale le cose sono state sequestrate e quella che avrebbe diritto alla loro restituzione possono proporre, entro dieci giorni dalla notifica del decreto ovvero dalla diversa data in cui l'interessato ha avuto conoscenza dell'avvenuto sequestro, richiesta di riesame, anche nel merito, a norma dell'articolo 324.	<i>Identico.</i>
4. La richiesta di riesame non sospende l'esecuzione del provvedimento.	<i>Identico.</i>
Art. 415-bis (Avviso all'indagato della conclusione delle indagini preliminari)	Art. 415-bis (idem)
	[articolo 2, comma 1, lett. o)]
1. Prima della scadenza del termine previsto dal comma 2 dell'articolo 405, anche se prorogato, il pubblico ministero, se non deve formulare richiesta di archiviazione ai sensi degli articoli 408 e 411, fa notificare alla persona sottoposta alle indagini e al difensore nonché, quando si procede per i reati di cui agli articoli 572 e 612-bis del codice penale, anche al difensore della persona offesa o, in mancanza di questo, alla persona offesa avviso della conclusione delle indagini preliminari.	<i>Identico.</i>
2. L'avviso contiene la sommaria enunciazione del fatto per il quale si	<i>Identico.</i>

Codice di procedura penale	
Testo vigente	Testo come modificato dall'A.C. 1822
procede, delle norme di legge che si assumono violate, della data e del luogo del fatto, con l'avvertimento che la documentazione relativa alle indagini espletate è depositata presso la segreteria del pubblico ministero e che l'indagato e il suo difensore hanno facoltà di prenderne visione ed estrarne copia.	
2-bis. Qualora non si sia proceduto ai sensi dell'articolo 268, commi 4, 5 e 6, l'avviso contiene inoltre l'avvertimento che l'indagato e il suo difensore hanno facoltà di esaminare per via telematica gli atti depositati relativi ad intercettazioni ed ascoltare le registrazioni ovvero di prendere cognizione dei flussi di comunicazioni informatiche o telematiche e che hanno la facoltà di estrarre copia delle registrazioni o dei flussi indicati come rilevanti dal pubblico ministero. Il difensore può, entro il termine di venti giorni, depositare l'elenco delle ulteriori registrazioni ritenute rilevanti e di cui chiede copia. Sull'istanza provvede il pubblico ministero con decreto motivato. In caso di rigetto dell'istanza o di contestazioni sulle indicazioni relative alle registrazioni ritenute rilevanti il difensore può avanzare al giudice istanza affinché si proceda nelle forme di cui all'articolo 268, comma 6.	<i>Identico.</i>
	2-ter. L'avviso contiene altresì l'avvertimento che l'indagato e il suo difensore hanno facoltà di esaminare i dati, le informazioni e i programmi oggetto di sequestro ai sensi dell'articolo 254-ter, comma 12, e il diritto alla trasposizione dei dati, delle informazioni o dei programmi medesimi su supporto idoneo. Il difensore può, entro il termine di venti giorni, esaminare il duplicato e depositare richiesta motivata di sequestro dei dati, delle informazioni e dei programmi specificamente indicati come rilevanti in relazione alle circostanze di tempo e di luogo del fatto

Codice di procedura penale	
Testo vigente	Testo come modificato dall'A.C. 1822
	e alle modalità della condotta, nel rispetto dei criteri di necessità e proporzione. Sull'istanza provvede il pubblico ministero con decreto motivato. Ove il pubblico ministero ritenga che non si debba disporre il sequestro, si applica l'articolo 368. Quando la richiesta riguarda dati inerenti a comunicazioni, conversazioni o corrispondenza informatica inviate e ricevute, il pubblico ministero trasmette sempre l'istanza ai sensi dell'articolo 368 e il giudice provvede ai sensi dell'articolo 254-ter, comma 12, secondo e terzo periodo.
3. L'avviso contiene altresì l'avvertimento che l'indagato ha facoltà, entro il termine di venti giorni, di presentare memorie, produrre documenti, depositare documentazione relativa ad investigazioni del difensore, chiedere al pubblico ministero il compimento di atti di indagine, nonché di presentarsi per rilasciare dichiarazioni ovvero chiedere di essere sottoposto ad interrogatorio. Se l'indagato chiede di essere sottoposto ad interrogatorio il pubblico ministero deve procedervi. Con l'avviso l'indagato e la persona offesa alla quale lo stesso è notificato sono altresì informati che hanno facoltà di accedere ai programmi di giustizia riparativa.	<i>Identico.</i>
4. Quando il pubblico ministero, a seguito delle richieste dell'indagato, dispone nuove indagini, queste devono essere compiute entro trenta giorni dalla presentazione della richiesta. Il termine può essere prorogato dal giudice per le indagini preliminari, su richiesta del pubblico ministero, per una sola volta e per non più di sessanta giorni.	<i>Identico.</i>
5. Le dichiarazioni rilasciate dall'indagato, l'interrogatorio del medesimo ed i nuovi atti di indagine del pubblico ministero, previsti dai commi 3 e 4, sono utilizzabili se compiuti entro il termine stabilito dal	<i>Identico.</i>

Codice di procedura penale	
Testo vigente	Testo come modificato dall'A.C. 1822
comma 4, ancorché sia decorso il termine stabilito dalla legge o prorogato dal giudice	
Art. 431 (<i>Fascicolo per il dibattimento</i>)	Art. 431 (<i>idem</i>)
	[articolo 2, comma 1, lett. p)]
1. Immediatamente dopo l'emissione del decreto che dispone il giudizio, il giudice provvede nel contraddittorio delle parti alla formazione del fascicolo per il dibattimento. Se una delle parti ne fa richiesta il giudice fissa una nuova udienza, non oltre il termine di quindici giorni, per la formazione del fascicolo. Nel fascicolo per il dibattimento sono raccolti: a) gli atti relativi alla procedibilità dell'azione penale e all'esercizio dell'azione civile; b) i verbali degli atti non ripetibili compiuti dalla polizia giudiziaria; c) i verbali degli atti non ripetibili compiuti dal pubblico ministero; d) i documenti acquisiti all'estero mediante rogatoria internazionale e i verbali degli atti non ripetibili assunti con le stesse modalità; e) i verbali degli atti assunti nell'incidente probatorio; f) i verbali degli atti, diversi da quelli previsti dalla lettera d), assunti all'estero a seguito di rogatoria internazionale ai quali i difensori sono stati posti in grado di assistere e di esercitare le facoltà loro consentite dalla legge italiana; g) il certificato generale del casellario giudiziario e gli altri documenti indicati nell'articolo 236, nonché, quando si procede nei confronti di un apolide, di una persona della quale è ignota la cittadinanza, di un cittadino di uno Stato non appartenente all'Unione europea ovvero di un cittadino di uno Stato membro dell'Unione europea privo del codice fiscale o che è attualmente, o è	1. Immediatamente dopo l'emissione del decreto che dispone il giudizio, il giudice provvede nel contraddittorio delle parti alla formazione del fascicolo per il dibattimento. Se una delle parti ne fa richiesta il giudice fissa una nuova udienza, non oltre il termine di quindici giorni, per la formazione del fascicolo. Nel fascicolo per il dibattimento sono raccolti: a) gli atti relativi alla procedibilità dell'azione penale e all'esercizio dell'azione civile; b) i verbali degli atti non ripetibili compiuti dalla polizia giudiziaria; c) i verbali degli atti non ripetibili compiuti dal pubblico ministero; d) i documenti acquisiti all'estero mediante rogatoria internazionale e i verbali degli atti non ripetibili assunti con le stesse modalità; e) i verbali degli atti assunti nell'incidente probatorio; f) i verbali degli atti, diversi da quelli previsti dalla lettera d), assunti all'estero a seguito di rogatoria internazionale ai quali i difensori sono stati posti in grado di assistere e di esercitare le facoltà loro consentite dalla legge italiana; g) il certificato generale del casellario giudiziario e gli altri documenti indicati nell'articolo 236, nonché, quando si procede nei confronti di un apolide, di una persona della quale è ignota la cittadinanza, di un cittadino di uno Stato non appartenente all'Unione europea ovvero di un cittadino di uno Stato membro dell'Unione europea privo del codice fiscale o che è attualmente, o è

Codice di procedura penale	
Testo vigente	Testo come modificato dall'A.C. 1822
stato in passato, titolare anche della cittadinanza di uno Stato non appartenente all'Unione europea, una copia del cartellino fotodattiloscopico con indicazione del codice univoco identificativo; <i>h)</i> il corpo del reato e le cose pertinenti al reato, qualora non debbano essere custoditi altrove.	stato in passato, titolare anche della cittadinanza di uno Stato non appartenente all'Unione europea, una copia del cartellino fotodattiloscopico con indicazione del codice univoco identificativo; <i>h)</i> il corpo del reato e le cose pertinenti al reato e, in ogni caso, i supporti di cui all'articolo 254-ter, comma 13, qualora non debbano essere custoditi altrove.
	1-bis. Ai fini indicati dal comma 1 e fermo quanto previsto dal comma 2, il giudice dispone la trascrizione integrale delle conversazioni o comunicazioni e la stampa in forma intellegibile delle comunicazioni informatiche o telematiche oggetto di sequestro ai sensi degli articoli 254-ter, comma 12, e 415-bis, comma 2-ter, secondo, terzo, quarto e quinto periodo. Si osservano le forme, i modi e le garanzie previste per l'espletamento delle perizie.
2. Le parti possono concordare l'acquisizione al fascicolo per il dibattimento di atti contenuti nel fascicolo del pubblico ministero, nonché della documentazione relativa all'attività di investigazione difensiva.	<i>Identico.</i>
Art. 454 (Presentazione della richiesta del pubblico ministero)	Art. 454 (idem)
	[articolo 2, comma 1, lett. q)]
1. Entro novanta giorni dalla iscrizione della notizia di reato nel registro previsto dall'articolo 335, il pubblico ministero trasmette la richiesta di giudizio immediato alla cancelleria del giudice per le indagini preliminari.	<i>Identico.</i>
2. Con la richiesta è trasmesso il fascicolo contenente la notizia di reato, la documentazione relativa alle indagini espletate e i verbali degli atti compiuti davanti al giudice per le indagini	<i>Identico.</i>

Codice di procedura penale	
Testo vigente	Testo come modificato dall'A.C. 1822
preliminari. Il corpo del reato e le cose pertinenti al reato, sono allegati al fascicolo, qualora non debbano essere custoditi altrove.	
2-bis. Qualora non abbia proceduto ai sensi dell'articolo 268, commi 4, 5 e 6, con la richiesta il pubblico ministero deposita l'elenco delle intercettazioni di comunicazioni o conversazioni o dei flussi di comunicazioni informatiche o telematiche rilevanti ai fini di prova. Entro quindici giorni dalla notifica prevista dall'articolo 456, comma 4, il difensore può depositare l'elenco delle ulteriori registrazioni ritenute rilevanti e di cui chiede copia. Sull'istanza provvede il pubblico ministero con decreto motivato. In caso di rigetto dell'istanza o di contestazioni sulle indicazioni relative alle registrazioni ritenute rilevanti il difensore può avanzare al giudice istanza affinché si proceda nelle forme di cui all'articolo 268, comma 6. Il termine di cui al presente comma può essere prorogato di dieci giorni su richiesta del difensore.	<i>Identico.</i>
	2-ter. Entro il medesimo termine di cui al comma 2-bis, secondo periodo, il difensore può esaminare il duplicato informatico conservato ai sensi dell'articolo 254-ter, comma 16, ai fini dell'eventuale richiesta di cui all'articolo 415-bis, comma 2-ter, secondo periodo, da formulare in sede di richieste di giudizio abbreviato di cui all'articolo 438, comma 5, ovvero di ammissione di prove di cui all'articolo 493.
Art. 461 (<i>Opposizione</i>)	Art. 461 (<i>idem</i>)
	[articolo 2, comma 1, lett. r)]
1. Nel termine di quindici giorni dalla notificazione del decreto, l'imputato e la persona civilmente obbligata per la pena pecuniaria, personalmente o a mezzo del difensore eventualmente nominato,	<i>Identico.</i>

Codice di procedura penale	
Testo vigente	Testo come modificato dall'A.C. 1822
possono proporre opposizione con le forme previste dall'articolo 582 nella cancelleria del giudice per le indagini preliminari che ha emesso il decreto ovvero nella cancelleria del tribunale o del giudice di pace del luogo in cui si trova l'opponente.	
	1-bis. Entro il medesimo termine di cui al comma 1, il difensore può esaminare il duplicato informatico conservato ai sensi dell'articolo 254-ter, comma 16, ai fini dell'eventuale richiesta di cui all'articolo 415-bis, comma 2-ter, secondo periodo, da formulare in sede di richieste di giudizio abbreviato di cui all'articolo 438, comma 5, ovvero di ammissione di prove di cui all'articolo 493.
2. La dichiarazione di opposizione deve indicare, a pena di inammissibilità, gli estremi del decreto di condanna, la data del medesimo e il giudice che lo ha emesso. Ove non abbia già provveduto in precedenza, nella dichiarazione l'opponente può nominare un difensore di fiducia.	<i>Identico.</i>
3. Con l'atto di opposizione l'imputato può chiedere al giudice che ha emesso il decreto di condanna il giudizio immediato ovvero il giudizio abbreviato o l'applicazione della pena a norma dell'articolo 444.	<i>Identico.</i>
4. L'opposizione è inammissibile, oltre che nei casi indicati nel comma 2, quando è proposta fuori termine o da persona non legittimata.	<i>Identico.</i>
5. Se non è proposta opposizione o se questa è dichiarata inammissibile, il giudice che ha emesso il decreto di condanna ne ordina l'esecuzione.	<i>Identico.</i>
6. Contro l'ordinanza di inammissibilità l'opponente può proporre ricorso per cassazione.	<i>Identico.</i>

