*Il Ministro della Giustizia*

**VISTO** il decreto del Presidente della Repubblica 22 settembre 1988, n. 447, recante approvazione del codice di procedura penale;

**VISTO** il decreto legislativo 28 luglio 1989, n. 271, recante norme di attuazione, di coordinamento e transitorie del codice di procedura penale;

**VISTA** la legge 23 giugno 2017, n. 103, recante modifiche al codice penale, al codice di procedura penale e all'ordinamento penitenziario;

**VISTA** la legge 25 ottobre 2017, n. 163, recante delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea – Legge di delegazione europea 2016-2017 – e, in particolare, l'art. 11 relativo all'attuazione della direttiva (UE) 2016/680;

**VISTO** il decreto legislativo 29 dicembre 2017, n. 216, recante disposizioni in materia di intercettazioni di conversazioni o comunicazioni, in attuazione della delega di cui all'articolo 1, commi 82, 83 e 84, lettere a), b), c), d) ed e), della legge 23 giugno 2017, n. 103;

**VISTO** l'articolo 2, comma 2, del decreto del Ministro della Giustizia 20 aprile 2018, recante disposizioni di attuazione per le intercettazioni mediante inserimento di captatore informatico e per l'accesso all'archivio informatico a norma dell'articolo 7, commi 1 e 3, del decreto legislativo 29 dicembre 2017, n. 216;

**VISTO** il decreto-legge 10 agosto 2023, n. 105, convertito con modificazioni dalla legge 9 ottobre 2023, n. 137, recante disposizioni urgenti in materia di processo penale, di processo civile, di contrasto agli incendi boschivi, di recupero dalle tossicodipendenze, di salute e di cultura, nonché in materia di personale della magistratura e della pubblica amministrazione;

**VISTO** il decreto del Ministro della Giustizia 6 ottobre 2023, adottato ai sensi dell'articolo 2, comma 2, del decreto-legge 10 agosto 2023, n. 105;

**VISTO** il decreto del Ministro della Giustizia 5 gennaio 2024, adottato ai sensi dell'articolo 2, comma 3, del decreto-legge 10 agosto 2023, n. 105;

**VISTI** in particolare i commi 5 e 6 dell'art. 2 del decreto-legge 10 agosto 2023, n. 105, a tenore dei quali con decreto del Ministro della Giustizia è disposta l'attivazione presso le infrastrutture interdistrettuali digitali dell'archivio digitale di cui agli articoli 269, comma 1, del codice di procedura penale e 89-*bis* delle disposizioni di attuazione del codice di procedura penale e sono definiti i tempi, le modalità e i requisiti di sicurezza della migrazione e del conferimento;

**VISTO** il decreto legislativo del 7 marzo 2005 n. 82 e successive modificazioni, recante Codice dell'amministrazione digitale (CAD) e successive modifiche;

**VISTO** il decreto legislativo 30 giugno 2003, n. 196, recante Codice in materia di protezione dei dati personali e successive modifiche;

**VISTA** la direttiva (UE) 2022/2555 del parlamento europeo e del consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (c.d. direttiva NIS 2);

**VISTO** il decreto legislativo 18 maggio 2018, n. 51 recante attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio;

**VISTO** il decreto-legge 21 settembre 2019, n. 105, convertito con modificazioni dalla legge 18 novembre 2019, n. 133, recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica;

**SENTITI** il Consiglio superiore della magistratura, il Garante per la protezione dei dati personali e il Comitato interministeriale per la cybersicurezza;

**D E C R E T A**

## Articolo 1

*(Definizioni)*

1. Agli effetti del presente decreto si intende per:

   a) «area di *staging*»: area di memoria non volatile utilizzata in via temporanea per ricevere, presso le infrastrutture digitali interdistrettuali, i dati oggetto di migrazione e processarli (e.g., calcolo dell'integrità e ulteriore cifratura) prima di caricarli definitivamente;

b) «*storage*»: conservazione delle informazioni tramite una tecnologia sviluppata appositamente per conservarle e renderle accessibili secondo necessità;
c) «*hash* crittografico»: funzione deterministica e non invertibile che mappa un dato arbitrario in input in una stringa di lunghezza predefinita;
d) «meccanismo di autenticazione del dato»: processo che consente di associare ad un dato il relativo *hash* crittografico, generato anche utilizzando in ingresso alla funzione di *hash* uno o più segreti di natura simmetrica;
e) «crittografia dei dati *at-rest*»: applicazione di algoritmi crittografici al fine di cifrare dati e informazioni memorizzati su dispositivi di archiviazione non volatili, con l'obiettivo di garantire la riservatezza delle informazioni non soltanto quando i dati vengono utilizzati ma anche quando essi sono "a riposo" (*at rest*), ossia quando i supporti fisici su cui sono memorizzati sono spenti o accesi ma inutilizzati;
f) «autenticità»: capacità di identificare con certezza la provenienza di dati e informazioni, ossia verificare l'identità dell'origine;
g) «integrità»: caratteristica relativa alla necessità per dati e informazioni memorizzate in un sistema o scambiate tra due entità di essere protette da modifiche non autorizzate;
h) «riservatezza»: accessibilità a dati e informazioni solo da parte di utenti e processi che ne hanno diritto, in base alle *policy* definite nel sistema;
i) «SSD (*Solid state drive*)»: dispositivi di memoria di massa che si contraddistinguono perché in grado di memorizzare grandi quantità di dati in modo non volatile senza servirsi di parti meccaniche;
j) «*hard disk*»: dispositivo di memoria che utilizza uno o più dischi magnetizzati per l'archiviare dati e applicazioni;
k) «RAID (*Redundant Array of Indipendent Disc*)»: tecnologia che combina più dischi rigidi utilizzati per memorizzare dati e garantire ridondanza e migliori prestazioni nella gestione degli stessi;
l) «*seed*»: è un valore numerico utilizzato per inizializzare un generatore di numeri pseudo-casuali (PRNG o CS-PRNG), ossia una funzione matematica che genera un numero (pseudo) casuale della lunghezza desiderata, spesso utilizzato per la generazione di una chiave crittografica;
m) «chiave simmetrica»: chiave utilizzata in input ad un algoritmo di cifratura di tipo simmetrico condivisa tra tutti gli utenti autorizzati ad eseguire l'algoritmo sul dato trattato;
n) «AES (*Advanced Encryption Standard*)»: algoritmo di cifratura a chiave simmetrica, il blocco è di dimensione fissa e la chiave può essere di 128, 192 o 256 bit;
o) «*Active Directory* (AD)»: sistema commerciale che consente di catalogare, raggruppandoli secondo la struttura organizzativa, risorse, servizi e utenti all'interno di "domini" e di gestire l'autenticazione degli utenti;

p) «RBAC (*role-based access control*)»: tecnica di controllo di accesso degli utenti alle risorse di un sistema informatico, incentrata sui concetti di ruolo e privilegio;
q) «istanza locale»: con riferimento all'archivio digitale delle intercettazioni, installazione del sistema, costituita dalla componente *software* e dalle relative basi di dati, operativa presso una specifica procura della Repubblica;
r) «metadati»: i registri di accesso e di utilizzo delle informazioni, nonché gli indici che consentono di reperire le intercettazioni memorizzate all'interno dell'archivio;
s) «DGSIA»: la Direzione generale per i sistemi informativi automatizzati del Dipartimento per la transizione digitale, l'analisi statistica e le politiche di coesione del Ministero della Giustizia.

**Articolo 2**

*(Oggetto e ambito di applicazione)*

1. Con il presente decreto, accertata la piena funzionalità delle infrastrutture digitali interdistrettuali istituite con il decreto del Ministro della Giustizia 6 ottobre 2023, è disposta l'attivazione dell'archivio digitale di cui agli articoli 269, comma 1, del codice di procedura penale e 89-*bis* delle disposizioni di attuazione del codice di procedura penale, di seguito denominato «archivio digitale delle intercettazioni» o «ADI».
2. Con il presente decreto è altresì autorizzata la migrazione dei dati dalle procure della Repubblica e il conferimento dei nuovi dati alle infrastrutture digitali interdistrettuali e ne sono fissati i tempi, le modalità e i requisiti di sicurezza.
3. Ferma restando l'applicazione delle misure di sicurezza di cui al regolamento adottato con decreto del Presidente del Consiglio dei ministri 14 aprile 2021, n. 81, con il presente decreto sono altresì dettagliate le ulteriori misure tecnico organizzative di funzionamento del sistema previste dall'articolo 6, comma 2, del decreto del Ministro della Giustizia 5 gennaio 2024.

**Articolo 3**

*(Data di attivazione dell'archivio presso le infrastrutture digitali interdistrettuali)*

1. L'ADI presso le infrastrutture digitali interdistrettuali istituite con il decreto del Ministro della Giustizia 6 ottobre 2023 è attivato a decorrere dal 1° marzo 2024.

**Articolo 4**

*(Tempi e modalità della migrazione dei dati verso le infrastrutture digitali interdistrettuali)*

1. Le operazioni di migrazione dei dati esistenti dalle singole procure della Repubblica verso le infrastrutture digitali interdistrettuali sono effettuate dalla DGSIA, di intesa con i singoli procuratori della Repubblica, nel periodo compreso tra il 1° marzo 2024 e il 28 febbraio 2025.
2. I dati sono distribuiti all'interno dei sistemi di archiviazione installati presso le quattro sale server individuate dal decreto del Ministro della Giustizia 6 ottobre 2023. Per aspetti organizzativi ogni procura è assegnata ad una sala server dell'infrastruttura digitale interdistrettuale in base alla migliore prossimità geografica. In caso di indisponibilità temporanea della sala server più vicina, per il tempo del disservizio, la procura è assegnata alla seconda sala server in base alla migliore prossimità geografica.
3. Le operazioni di migrazione dei dati attengono ai verbali, agli atti e alle registrazioni delle intercettazioni cui afferiscono, nonché a tutti i metadati gestiti dall'istanza locale dell'archivio digitale delle intercettazioni presso la procura di riferimento, indispensabili per il corretto funzionamento del sistema.
4. Il processo di migrazione dei dati consiste nello spostamento, mediante realizzazione di apposita copia temporanea su un'area intermedia di *staging* sita presso la sala server di riferimento dell'infrastruttura digitale interdistrettuale, dei dati presenti nell'attuale istanza locale di ADI operativa presso una determinata procura della Repubblica verso l'infrastruttura digitale interdistrettuale.
5. La copia temporanea sull'area di *staging* di cui al comma 4 si configura esclusivamente in relazione alla necessità di applicare un ulteriore strato di cifratura a garanzia della confidenzialità dei dati. L'area di *staging* sita presso la sala server di riferimento dell'infrastruttura digitale interdistrettuale permette inoltre di facilitare e centralizzare le operazioni di riversamento, evitando la predisposizione di aree specifiche presso ciascuna procura in ottica di razionalizzazione delle risorse di *storage*.
6. Presso la sala server di riferimento dell'infrastruttura digitale interdistrettuale è creata una copia 1:1 di tutti i dati di competenza della procura sorgente, i quali sono processati e riversati nell'archivio centralizzato costituito dalle infrastrutture digitali interdistrettuali.

7. Per lo svolgimento delle operazioni di cui al comma 4 sono adottate misure tecniche e organizzative in grado di garantire l'integrità e la completezza dei dati oggetto di migrazione, mediante meccanismi di autenticazione del dato basati sul calcolo dell'*hash* crittografico prima e dopo le operazioni di copia, anche temporanea, tra le istanze locali e l'area di *staging* e tra quest'ultima e l'ADI e il successivo confronto di tali *hash*.
8. L'area di *staging* che conserva la copia temporanea dei dati migrati garantisce la cifratura di tutti i dati *at-rest*. Accertato il corretto completamento delle operazioni di riversamento sull'archivio centralizzato delle infrastrutture digitali interdistrettuali, l'intero contenuto afferente ai dati di cui al comma 3 viene eliminato, adottando tecniche di cancellazione sicura dei dati secondo le linee guida e gli standard nazionali e internazionali di riferimento, sia dall'archivio locale presso la procura che dall'area di *staging*.
9. Le operazioni di migrazione possono essere svolte con modalità telematiche o, quando la dimensione dei dati coinvolti lo richiede, con modalità non telematiche mediante trasferimento su supporti fisici. La scelta della modalità di migrazione è effettuata sulla base delle specifiche condizioni tecniche in essere presso ogni procura della Repubblica, sempre d'intesa con il procuratore della Repubblica.
10. Accertato il completamento delle operazioni di migrazione attuate mediante supporti fisici gli stessi verranno distrutti.

**Articolo 5**

*(Requisiti di sicurezza delle operazioni di migrazione)*

1. Le operazioni di migrazione dei dati da ciascun archivio digitale delle intercettazioni presente nella procura della Repubblica ad ADI sono condotte garantendo, per tutta la durata delle attività, la riservatezza, l'integrità e l'autenticità dei dati trasferiti.
2. In caso di migrazione con modalità non telematiche i dati devono essere trasferiti mediante l'utilizzo di appositi dispositivi di memorizzazione (dischi SSD), adottando misure tecniche e organizzative in grado di garantire l'integrità e la completezza dei dati, analoghe a quelle previste in caso di migrazione con modalità telematiche. Accertato il corretto completamento delle operazioni di riversamento sull'archivio centralizzato delle infrastrutture digitali interdistrettuali, l'intero contenuto presente sui dispositivi di memorizzazione viene eliminato, adottando

tecniche di cancellazione sicura dei dati secondo le linee guida e gli standard nazionali e internazionali di riferimento ovvero mediante distruzione fisica del dispositivo stesso.

3. Il dispositivo utilizzato per la migrazione con modalità non telematiche dei dati garantisce un elevato livello di affidabilità. Sono adottate configurazioni che ridondino i dati da trasferire, in modo da consentire la migrazione anche nel caso in cui uno degli oggetti su cui i dati sono memorizzati cessi di funzionare durante l'attività di trasferimento.
4. La migrazione con modalità non telematiche è protetta cifrando i dati da trasferire mediante algoritmo simmetrico del tipo AES-128 o AES-256. La cifratura dei dati avviene prima che il supporto fisico utilizzato per la migrazione esca dai locali della procura ed è eseguita da personale tecnico incaricato dal procuratore della Repubblica o da un suo delegato.
5. La chiave simmetrica utilizzata per le operazioni di cifratura di cui al comma 4 è diversa per ciascuna operazione di migrazione. La chiave è generata all'interno del medesimo dispositivo deputato a svolgere la cifratura dei dati ed è caratterizzata da elevata entropia.
6. La chiave simmetrica è nota esclusivamente al personale tecnico di cui al comma 4 che avvia la migrazione presso la procura della Repubblica e la completa presso le infrastrutture digitali interdistrettuali, nel rispetto di procedure formalizzate e uniformi a livello nazionale. La chiave può essere allegata ai dati migrati esclusivamente in forma cifrata mediante ulteriore chiave crittografica, oppure, se la chiave viene generata a partire da un seme (*seed*), il mittente può condividerlo in maniera sicura con il destinatario dividendo l'informazione in due parti e comunicando ciascuna di esse mediante un canale sicuro distinto.
7. La migrazione con modalità telematiche è avviata da personale tecnico incaricato dalla DGSIA. Il canale di comunicazione utilizzato per la migrazione dei dati è cifrato mediante l'utilizzo di tecniche crittografiche allo stato dell'arte per la protezione dei dati "in transito", tenendo conto delle specifiche Linee guida adottate dall'Agenzia per la cybersicurezza nazionale, garantisce la autenticazione degli attori coinvolti e implementa meccanismi per assicurare l'integrità e autenticità delle comunicazioni.
8. Tutte le operazioni di migrazione avvengono alla presenza di personale incaricato dal procuratore della Repubblica o da un suo delegato. Delle operazioni eseguite durante la migrazione viene redatto processo verbale formato da personale amministrativo o di polizia giudiziaria designato dal procuratore della Repubblica.

**Articolo 6**

*(Tempi, modalità e requisiti di sicurezza del conferimento verso le infrastrutture digitali interdistrettuali)*

1. Le operazioni di conferimento dei dati verso le infrastrutture digitali interdistrettuali sono effettuate dalle singole procure della Repubblica a partire dal giorno successivo all'avvio delle operazioni di migrazione di cui all'articolo 4.
2. Fermo restando quanto previsto dagli articoli 1, comma 1, lettera f), 2, comma 5, lettera a), e 3, comma 1, del decreto del Ministro della Giustizia 5 gennaio 2024, le modalità del conferimento prevedono:
    a) il trasferimento dei dati e delle informazioni relativi alle intercettazioni dagli impianti di registrazione dei fornitori a ADI, attraverso una rete telematica che colleghi, in ciascuna procura, i suddetti impianti di registrazione con le apparecchiature della procura;
    b) il trasferimento telematico dagli impianti della procura all'archivio centralizzato sulle infrastrutture digitali interdistrettuali.
3. Qualora presso le procure sussistano particolari condizioni di natura tecnica, anche con riferimento all'organizzazione degli edifici, che impediscano o ostacolino la realizzazione della rete telematica di cui al comma 2, lettera a), il trasferimento delle intercettazioni dagli impianti di registrazione dei fornitori a ADI potrà avvenire attraverso l'utilizzo di supporti fisici, che rispettano tutti i requisiti di sicurezza di cui all'articolo 5.
4. Per le operazioni di conferimento, così come per tutte le altre operazioni consentite da ADI, gli utenti accedono, mediante protocollo cifrato, ad una delle quattro istanze del *software* installate rispettivamente presso le quattro sale server individuate dal decreto del Ministro della Giustizia 6 ottobre 2023, secondo criteri di prossimità geografica e condizioni di carico sulla rete. Tali criteri consentono la distribuzione del traffico di rete anche in caso di indisponibilità di una o più istanze.
5. I requisiti di sicurezza delle operazioni di conferimento sono stabiliti nel rispetto dell'articolo 25 del decreto legislativo 18 maggio 2018, n. 51, e garantiscono la protezione, la disponibilità, l'accessibilità, l'integrità e la riservatezza dei dati e la continuità operativa dei sistemi e delle infrastrutture.
6. I requisiti di disponibilità dei dati e continuità operativa dei sistemi e delle infrastrutture sono definiti dall'articolo 2, comma 4, del decreto del Ministro della Giustizia 5 gennaio 2024.

7. I requisiti di protezione, integrità e riservatezza dei dati sono definiti dagli articoli 3 e 4 del decreto del Ministro della Giustizia 5 gennaio 2024.
8. I requisiti di accessibilità delle operazioni di conferimento sono conformi alle disposizioni delle Linee guida sull'accessibilità degli strumenti informatici emanate dall'Agenzia per l'Italia Digitale.

**Articolo 7**

*(Misure tecnico-organizzative di funzionamento del sistema)*

1. Le infrastrutture digitali interdistrettuali sono organizzate in modo da garantire la sicurezza fisica delle apparecchiature che compongono l'ADI. Gli accessi fisici agli ambienti ove sono installati i componenti dell'ADI sono regolamentati mediante un registro degli accessi.
2. L'ADI è organizzato in modo da garantire la segmentazione logica dei dati trattati rispetto a ogni singola procura della Repubblica. Gli accessi amministrativi ai vari componenti dell'ADI sono regolamentati e protetti da autenticazione a due fattori e da un sistema di *log* che consenta di ricostruire tutte le operazioni effettuate in modo da tracciare in maniera non modificabile le azioni di chi svolge attività di tipo sistemistico e manutentivo.
3. I sistemi informatici costituenti le infrastrutture digitali interdistrettuali non hanno accesso ai dati in chiaro delle intercettazioni, poiché li ricevono in forma già cifrata, né hanno accesso alla chiave di decifratura. Presso le infrastrutture digitali interdistrettuali sono presenti in chiaro solo i metadati che non contengono informazioni sensibili e devono necessariamente rimanere in chiaro per il corretto funzionamento del sistema.
4. Il collegamento telematico tra le procure della Repubblica e le infrastrutture digitali interdistrettuali è realizzato mediante canali sicuri, ove i dati transitano in forma cifrata. I canali suddetti garantiscono inoltre l'integrità dei dati mediante appositi meccanismi per rilevare qualsiasi indebita modifica sulle informazioni in transito.
5. I componenti sia *hardware* sia *software* che costituiscono l'architettura di ADI relativamente ai punti di rete ai sensi dell'articolo 1, comma 2, del decreto del Ministro della Giustizia 6 ottobre 2023, indispensabili per il corretto funzionamento del sistema, sono installati in un locale tecnico dedicato presente presso ciascuna procura della Repubblica. L'accesso fisico a tale locale è regolamentato da appositi

controlli ed è correlato ad un sistema di tracciamento atto a registrare tutte le operazioni effettuate.

6. L'accesso in chiaro ai dati delle intercettazioni si realizza esclusivamente presso la procura della Repubblica di competenza, mediante l'impiego dei componenti di cui al comma 5. Tali componenti sono progettati espressamente per poter eseguire gli algoritmi di crittografia simmetrici e asimmetrici necessari per accedere ai dati e sono gli unici elementi del sistema ADI ad aver accesso fisico alla chiave crittografica necessaria per decifrare i contenuti delle intercettazioni.
7. Le operazioni di accesso ai contenuti di cui al comma 6 vengono effettuate attraverso i componenti di cui al comma 5 esclusivamente nei casi di accesso previsti dall'articolo 89-*bis*, comma 3, delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, ovvero nei casi di esportazione dei dati verso altra procura. Le operazioni di accesso vengono eseguite esclusivamente in risposta a comandi provenienti da un apposito applicativo, previa verifica dell'identità dell'utente e della relativa autorizzazione ad eseguire determinate operazioni.
8. L'accesso all'applicativo di cui al comma 7 e alle sue funzionalità è consentito alle figure censite su *Active Directory* Nazionale (ADN) e profilate nel contesto di sicurezza applicativo, delineato sulla base del personale autorizzato all'accesso e del relativo modello RBAC (*role-based access control*) che consente di regolamentare ruoli e autorizzazioni dei vari utenti.

**Articolo 8**

*(Trattamento dei dati personali)*

1. Nell'ambito dei procedimenti che richiedono l'esecuzione di intercettazioni nei casi previsti dal codice di procedura penale, titolare del trattamento dei dati è la procura della Repubblica che procede, mentre il Ministero è responsabile del trattamento ai soli fini dell'allestimento e della manutenzione delle infrastrutture digitali interdistrettuali, comprendente l'attivazione del nuovo archivio centralizzato, garantendo l'autonomia del procuratore della Repubblica nell'esercizio delle funzioni di direzione, organizzazione e sorveglianza sulle attività di intercettazione e sui relativi dati e, in ogni caso, con esclusione dell'accesso ai dati in chiaro.
2. Il trattamento di dati è svolto al fine di assicurare i più elevati e uniformi livelli di sicurezza, aggiornamento tecnologico, efficienza, economicità e capacità di

risparmio energetico dei sistemi informativi funzionali alle attività di intercettazione eseguite da ciascun ufficio del pubblico ministero, consentendo alle procure della Repubblica il perseguimento delle seguenti finalità:

a. conferimento o trasferimento degli eventi e dei metadati che costituiscono le intercettazioni nel nuovo archivio centralizzato, in grado di garantire una maggiore efficienza nella gestione delle risorse;
b. consultazione delle intercettazioni da parte del 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, ai sensi dell'art. 89-*bis*, comma 3, delle disposizioni di attuazione del codice di procedura penale;
c. consultazione delle intercettazioni da parte dei difensori delle parti, successivamente alla notifica del deposito delle stesse presso il nuovo archivio centralizzato, al fine di valutare il contenuto delle intercettazioni nell'interesse degli assistiti, ai sensi dell'art. 89-*bis*, comma 5, delle disposizioni di attuazione del codice di procedura;
d. rilascio di copie delle intercettazioni a beneficio dei difensori o di eventuali altri uffici giudiziari autorizzati all'accesso ai contenuti, consentendo la consultazione dei contenuti in un secondo momento, a norma degli articoli 268, 415-*bis* e 454 del codice di procedura penale;
e. trasferimento per competenza verso altra procura, anche contestualmente al conferimento dell'intercettazione, nel caso in cui la competenza di una determinata indagine passi ad una diversa procura.

3. Il Ministero è responsabile del trattamento di dati personali effettuati nell'ambito dell'allestimento e della manutenzione delle infrastrutture digitali interdistrettuali per le intercettazioni per conto delle procure della Repubblica ai sensi del dell'articolo 18 del decreto legislativo 18 maggio 2018, n. 51.
4. Il Ministero si avvale di soggetti fornitori di tecnologie e servizi funzionali all'allestimento e alla manutenzione delle infrastrutture digitali interdistrettuali per le intercettazioni, sulla base di quanto disposto dell'articolo 18, commi 2 e 3, lettera f), del decreto legislativo 18 maggio 2018, n. 51, tra cui:
   a. gestione e manutenzione del servizio *identity management* del Ministero;
   b. gestione e manutenzione dei database;
   c. gestione e conduzione applicativa;

d. manutenzione della soluzione di conservazione centralizzata delle intercettazioni per ciò che concerne le componenti ospitate presso le infrastrutture digitali interdistrettuali;
e. installazione e gestione degli apparati di rete nell'ambito delle infrastrutture digitali interdistrettuali;
f. gestione dei *firewall* di rete presso le infrastrutture digitali interdistrettuali;
g. gestione e manutenzione delle componenti *hardware* e *software* installati presso le procure delle Repubblica, inclusi eventuali apparati di rete, atti ad interfacciarsi sia con i fornitori dei servizi di intercettazione sia con il sistema soluzione di conservazione centralizzata, nell'ambito delle finalità di trattamento di dati perseguite dalle procure delle Repubblica.

Il presente decreto verrà pubblicato nel Bollettino Ufficiale del Ministero della Giustizia.

Roma,

Il Ministro
Carlo Nordio

CARLO
NORDIO
26.02.2024
13:18:42
GMT+01:00