MINISTERO DELL'INTERNO

DECRETO 12 luglio 2023, n. **114**.

Regolamento concernente le modalità di funzionamento, accesso, consultazione del sistema di tracciabilità delle armi e delle munizioni, istituito ai sensi dell'articolo 11, del decreto legislativo 10 agosto 2018, n. 104.

IL MINISTRO DELL'INTERNO

DI CONCERTO CON

IL MINISTRO DELL'ECONOMICA E DELLE FINANZE

Visto l'articolo 117, secondo comma, lettera *h)* della Costituzione;

Visto l'articolo 17, comma 3, della legge 23 agosto 1988, n. 400;

Visto l'articolo 11, comma 6, del decreto legislativo 10 agosto 2018, n. 104 che rimette all'adozione di un regolamento la disciplina delle modalità di funzionamento di un «sistema informatico dedicato» per la tracciabilità delle armi e delle munizioni, anche per ciò che concerne le procedure di accesso, di consultazione, di conservazione dei dati, nonché di collegamento con il Centro elaborazione dati di cui all'articolo 8 della legge 1° aprile 1981, n. 121;

Visto il regolamento UE n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE;

Vista la direttiva 91/477/CEE del Consiglio, del 18 giugno 1991, relativa al controllo dell'acquisizione e della detenzione di armi, come codificata dalla direttiva (UE) 2021/555 del Parlamento europeo e del Consiglio, del 24 marzo 2021;

Visto il regolamento delegato (UE) 2019/686 della Commissione, del 16 gennaio 2019, che stabilisce le modalità dettagliate, a norma della direttiva 91/477/CEE del Consiglio, per lo scambio sistematico con mezzi elettronici di informazioni relative al trasferimento di armi da fuoco nell'Unione;

Vista la legge 18 aprile 1975, n. 110 e, in particolare, gli articoli 5 e 25, recanti disposizioni per la tenuta del registro giornaliero previsto dall'articolo 55 del testo unico delle leggi di pubblica sicurezza di cui al regio decreto 18 giugno 1931, n. 773;

Vista la legge 1° aprile 1981, n. 121 e, in particolare, gli articoli 8, 9 e 10, che prevedono l'istituzione del Centro elaborazione dati nell'ambito del Dipartimento della pubblica sicurezza del Ministero dell'interno, disciplinando il regime degli accessi e dei controlli;

Vista la legge 26 marzo 2001, n. 128 e, in particolare, l'articolo 21, comma 1, che prevede che le Forze di polizia conferiscono senza ritardo al Centro elaborazione dati del Dipartimento della pubblica sicurezza, le notizie e le informazioni acquisite nel corso delle attività di prevenzione e repressione dei reati e di quelle amministrative;

Visto il decreto legislativo 30 dicembre 1992, n. 527, recante attuazione della direttiva 91/477/CEE relativa al controllo dell'acquisizione e della detenzione di armi;

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 testo unico delle leggi di pubblica sicurezza, di cui al regio decreto 18 giugno 1931, n. 773 e, in particolare, gli articoli 35 e 55, concernenti i registri delle operazioni giornaliere che devono essere detenuti e compilati, rispettivamente, dai soggetti di cui all'articolo 1-*bis*, comma 1, lettera *f)* e *g)* del decreto legislativo 30 dicembre 1992, n. 527, nonché dagli esercenti fabbriche, depositi o rivendite di esplodenti;

Visto il regio decreto 6 maggio 1940, n. 635, recante «Approvazione del regolamento per l'esecuzione del testo unico 18 giugno 1931, n. 773 delle leggi di pubblica sicurezza»;

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» e, in particolare, l'articolo 1 che istituisce il perimetro di sicurezza cibernetica;

Visto il decreto del Presidente della Repubblica 15 gennaio 2018, n. 15, e in particolare, l'articolo 5, concernente la configurazione dei sistemi informativi e dei programmi informatici utilizzati per il trattamento dei dati personali per finalità di polizia da parte di organi, uffici e comandi di polizia, nonché l'articolo 10, che definisce i termini di conservazione dei medesimi dati;

Visto il decreto del Ministro dell'interno 24 maggio 2017, pubblicato nella *Gazzetta Ufficiale* n. 145 del 24 agosto 2017, recante l'individuazione dei trattamenti di dati personali effettuati dal Centro elaborazione dati del Dipartimento della pubblica sicurezza o da Forze di polizia sui dati destinati a confluirvi, ovvero da organi di pubblica sicurezza o altri soggetti pubblici nell'esercizio delle attribuzioni conferite da disposizioni di legge o di regolamento, effettuati con strumenti elettronici e i relativi titolari, in attuazione dell'articolo 53, comma 3, del decreto legislativo 30 giugno 2003, n. 196;

Visto il decreto del Presidente del Consiglio dei ministri 14 aprile 2021, n. 81, recante «Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'articolo 1,

comma 2, lettera *b)*, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e di misure volte a garantire elevati livelli di sicurezza»;

Sentito il Garante per la protezione dei dati personali che ha espresso il proprio parere favorevole con deliberazione del 7 aprile 2022;

Udito il parere del Consiglio di Stato, espresso dalla Sezione consultiva per gli atti normativi nell'adunanza del 4 ottobre 2022;

Sentito il Ministro della difesa con nota del 27 febbraio 2023;

Udito il concerto del Ministro dell'economia e delle finanze acquisito in data 14 marzo 2023;

Vista la comunicazione al Presidente del Consiglio dei ministri, riscontrata con nota n. 4.3.13.3/2021/47 del 14 aprile 2023 del Dipartimento per gli affari giuridici e legislativi della Presidenza del Consiglio dei ministri;

ADOTTA
il seguente regolamento:

Capo I

DISPOSIZIONI GENERALI

Art. 1.

Oggetto

1. Il presente regolamento disciplina le modalità di funzionamento del «sistema informatico dedicato» per la tracciabilità delle armi e delle munizioni di cui all'articolo 11 del decreto legislativo 10 agosto 2018, n. 104, nonché le procedure secondo le quali gli armaioli di cui all'articolo 1-*bis*, comma 1, lettera *g)*, del decreto legislativo 30 dicembre 1992, n. 527 e gli intermediari di cui all'articolo 1-*bis*, comma 1, lettera *f)*, del medesimo decreto legislativo, nei casi contemplati dall'articolo 31-*bis*, comma 2, del testo unico delle leggi di pubblica sicurezza, di cui al regio decreto 18 giugno 1931, n. 773, immettono i dati relativi alle operazioni giornaliere riguardanti le armi e le munizioni, al fine di assolvere agli obblighi di registrazione e comunicazione previsti dagli articoli 35 e 55 del predetto testo unico delle leggi di pubblica sicurezza.

2. Il presente regolamento stabilisce inoltre le modalità di autenticazione, autorizzazione e registrazione degli accessi e delle operazioni effettuate nel predetto Sistema informatico, le modalità di conservazione sicura e di verifica di qualità dei dati nonché della loro protezione e trasmissione in caso di malfunzionamento, danneggiamento o di altri eventi accidentali o dolosi riguardanti il medesimo Sistema.

3. Il presente regolamento disciplina, altresì, le modalità di collegamento del predetto Sistema informatico, ai fini di consultazione e riscontro dei dati, con il Centro elaborazione dati di cui all'articolo 8 della legge 1° aprile 1981, n. 121.

Art. 2.

Definizioni

1. Ai fini del presente regolamento, si intende per:

a) «armi», le armi da fuoco e le armi diverse da quelle da fuoco;

b) «arma da fuoco», l'arma da fuoco, come definita dall'articolo 1-*bis*, comma 1, lettera *a)*, del decreto legislativo 30 dicembre 1992, n. 527, l'arma da fuoco per uso scenico di cui all'articolo 22, primo comma, della legge 18 aprile 1975, n. 110, nonché l'arma da fuoco antica, artistica o rara di importanza storica disciplinata dal decreto del Ministro dell'interno 14 aprile 1982, emanato ai sensi dell'articolo 10, settimo comma, della medesima legge n. 110 del 1975;

c) «arma diversa dalle armi da fuoco», l'arma comune da sparo ad aria o a gas compressi, lunga o corta, i cui proiettili erogano un'energia cinetica superiore a 7,5 joule, nonché l'arma da sparo con modesta capacità offensiva, funzionante a aria o a gas compressi, i cui proiettili erogano un'energia cinetica non superiore a 7,5 joule;

d) «armaiolo», l'operatore economico che esercita le attività in materia di armi da fuoco e munizioni indicate dall'articolo 1-*bis*, comma 1, lettera *g)*, del decreto legislativo n. 527 del 1992;

e) «autorità nazionale», l'autorità nazionale competente allo scambio delle informazioni in materia di trasferimenti, a titolo definitivo, di armi da fuoco, individuata nel competente Ufficio per l'Amministrazione generale del Dipartimento della pubblica sicurezza;

f) «CED», il Centro elaborazione dati di cui all'articolo 8 della legge 1° aprile 1981, n. 121;

g) «CEN», il Centro elettronico nazionale della Polizia di Stato per la gestione, il coordinamento e lo sviluppo degli archivi e delle procedure informatizzate;

h) «DIA», la Direzione investigativa antimafia, di cui all'articolo 108 del decreto legislativo 6 settembre 2011, n. 159;

i) «decreto legislativo n. 51 del 2018», il decreto legislativo 18 maggio 2018, n. 51;

l) «decreto legislativo n. 104 del 2018», il decreto legislativo 10 agosto 2018, n. 104;

m) «Dipartimento della pubblica sicurezza», il Dipartimento della pubblica sicurezza del Ministero dell'interno di cui all'articolo 4 della legge 1° aprile 1981, n. 121;

n) «Focal Point» il personale delle Forze di polizia di cui all'articolo 16, primo comma, della legge 1° aprile 1981, n. 121, incaricato della formazione e della gestione operativa degli utenti che accedono al SITAM;

o) «Forze di polizia», le Forze di polizia di cui all'articolo 16, primo comma, della legge 1° aprile 1981, n. 121 e successive modificazioni;

p) «intermediario», l'operatore economico che esercita le attività in materia di armi da fuoco e munizioni indicate dall'articolo 1-*bis*, comma 1, lett. *f)*, del decreto legislativo n. 527 del 1992;

q) «legge n. 110 del 1975», la legge 18 aprile 1975, n. 110;

r) «legge n. 121 del 1981», la legge 1° aprile 1981, n. 121;

s) «munizione», la munizione utilizzata in un'arma da fuoco come definita dall'articolo 1-*bis*, comma 1, lettera *d)* del predetto decreto legislativo n. 527 del 1992;

t) «parte d'arma», una delle componenti essenziali di un'arma da fuoco come definite dall'articolo 1-*bis*, comma 1, lettera *b)* del decreto legislativo n. 527 del 1992;

u) «Prefettura-UTG», la Prefettura – Ufficio territoriale del Governo;

v) «rappresentante», la persona fisica, dipendente dell'armaiolo, che abbia ottenuto l'approvazione della nomina a rappresentante del medesimo armaiolo ai sensi dell'articolo 8, secondo comma, TULPS;

z) «regolamento delegato (UE) 2019/686», il regolamento delegato (UE) 2019/686 della Commissione del 16 gennaio 2019;

aa) «replica di arma antica ad avancarica a colpo singolo», la replica di arma antica ad avancarica a colpo singolo di modello e/o tipologia anteriore al 1890, come definita all'articolo 12 del decreto ministeriale 9 agosto 2001, n. 362;

bb) «SITAM», il «*sistema informatico dedicato*» per la tracciabilità delle armi e delle munizioni, di cui all'articolo 11 del decreto legislativo 10 agosto 2018, n. 104;

cc) «TULPS», il testo unico delle leggi di pubblica sicurezza, di cui al regio decreto 18 giugno 1931, n. 773.

2. Ai fini del presente regolamento, si intende, inoltre, per:

a) «accesso», l'operazione di trattamento elettronico che consente di prendere visione e di estrarre copia, memorizzandola su qualunque tipo di supporto, dei dati conservati nel SITAM e di quelli riguardanti i detentori delle armi e delle munizioni conservati nel CED;

b) «aggiornamento», l'operazione di trattamento elettronico che consente di modificare o di cancellare, con modalità sicure, i dati già contenuti nel SITAM, nel rispetto dei principi stabiliti dall'articolo 3 del decreto legislativo n. 51 del 2018;

c) «amministratore locale SITAM», il dipendente della Polizia di Stato in servizio presso le Questure addetto alla gestione delle utenze per l'accesso al SITAM da parte degli utenti di cui al successivo punto *i)*;

d) «consultazione», l'operazione di trattamento elettronico che consente di accedere, nei limiti stabiliti dal relativo profilo di autorizzazione di cui al comma 3, lettera *h)*, alle informazioni conservate nel SITAM;

e) «immissione», l'operazione di trattamento elettronico che consente l'inserimento di dati nel SITAM, per le finalità per cui esso è istituito, nel rispetto dei principi stabiliti dall'articolo 3 del decreto legislativo n. 51 del 2018;

f) «interrogazione», l'operazione di collegamento telematico con il SITAM al fine di effettuare l'accesso, la consultazione, l'immissione o l'aggiornamento dei dati conservati nel SITAM;

g) «operatore», l'appartenente alle Forze di polizia di cui all'articolo 16, primo comma, della legge n. 121 del 1981, in servizio presso il Dipartimento della pubblica sicurezza, le Questure, gli uffici e comandi delle predette Forze di polizia, nei cui confronti sono state rilasciate le credenziali di autenticazione che consentono di effettuare le interrogazioni del SITAM;

h) «operatore dell'Amministrazione civile dell'interno», l'appartenente all'Amministrazione civile dell'interno in servizio presso il Dipartimento della pubblica sicurezza, le Prefetture-UTG, le Questure e gli uffici locali di pubblica sicurezza, nei cui confronti sono state rilasciate le credenziali di autenticazione che consentono l'accesso o la consultazione del SITAM;

i) «utente», l'armaiolo, il suo rappresentante o i dipendenti dell'armaiolo, nonché l'intermediario o i suoi dipendenti.

3. Ai fini del presente regolamento si intendono, altresì, per:

a) «autenticazione», l'insieme degli strumenti elettronici delle procedure per la verifica dell'identità dell'operatore, dell'operatore dell'Amministrazione civile dell'interno o dell'utente;

b) «autenticazione forte», metodo di autenticazione multifattore che si basa sull'utilizzo congiunto di due o più fattori di autenticazione individuale;

c) «casella di posta elettronica assegnata dall'Amministrazione», casella di posta elettronica istituzionale rilasciata all'operatore, all'operatore dell'Amministrazione civile dell'interno dall'Amministrazione o dall'ente di appartenenza;

d) «client», postazione di lavoro che accede ai servizi o alle risorse di un'altra componente servente;

e) «credenziali di autenticazione», i dati e i dispositivi in possesso dell'operatore, dell'operatore dell'Amministrazione civile dell'interno ovvero dell'utente, da questi conosciuti e ad essi univocamente correlati, necessari per l'autenticazione;

f) «login», la procedura di autenticazione per l'effettuazione di operazioni di trattamento all'interno del SITAM;

g) «password», sequenza di caratteri alfanumerici utilizzata per accedere in modo esclusivo a una risorsa informatica;

h) «profilo di autorizzazione», l'insieme delle informazioni univocamente associate all'operatore, all'operatore dell'Amministrazione civile dell'interno o all'utente che consente di individuare a quali dati conservati nel SITAM questi ultimi sono abilitati ad accedere, nonché quali trattamenti sono abilitati ad effettuare;

i) «sistema di autorizzazione», l'insieme degli strumenti e delle procedure che abilitano il trattamento dei dati del SITAM in funzione del profilo di autorizzazione

riconosciuto all'operatore, all'operatore dell'Amministrazione civile dell'interno ovvero all'utente, a seconda della categoria di soggetti cui esso appartiene o da cui dipende;

l) «URL», l'Uniform Resource Locator, sequenza di caratteri che identifica univocamente l'indirizzo di rete del SITAM;

m) «username», nome con il quale l'utente viene riconosciuto da un computer o da un programma informatico;

n) «violazione dei dati personali», la violazione della sicurezza che comporta colposamente o dolosamente la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

4. Ai fini del presente regolamento, si intendono, altresì, per:

a) «articolazione competente per la gestione del CED», l'articolazione del servizio per i Sistemi Informativi della Direzione centrale della polizia criminale del Dipartimento della pubblica sicurezza, competente per la gestione del CED;

b) «Direzione centrale della polizia criminale», la Direzione centrale della polizia criminale di cui all'articolo 4, comma 2, lettera *g)*, del decreto del Presidente del Consiglio dei ministri 11 giugno 2019, n. 78.

5. Infine, ai fini del presente regolamento, si intendono per:

a) «CIE», il documento di identità personale rilasciato dal Ministero dell'interno denominato «Carta di identità elettronica», come definito dall'articolo 1 del decreto legislativo 7 marzo 2005, n. 82 (CAD);

b) «Identità digitale», la rappresentazione informatica della corrispondenza biunivoca tra un utente e i suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale secondo le modalità di cui al decreto del Presidente del Consiglio dei ministri, in data 24 ottobre 2014, recante «*Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID), nonché dei tempi e delle modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese*» e dei suoi regolamenti attuativi;

c) «Identità digitale uso professionale», l'identità digitale SPID contenente un attributo che dichiara tale caratteristica, rilasciata secondo le linee guida di cui alla determina dell'AGID n. 318/2019;

d) «Regolamento UE 910/2014», il Regolamento UE n. 910/2014 del Parlamento europeo e del Consiglio del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE;

e) «SPID», il sistema pubblico dell'identità digitale, istituito ai sensi dell'articolo 64 del CAD, come modificato dall'articolo 17-*ter* del decreto-legge 21 giugno 2013, n. 69, convertito, con modificazioni, dalla legge 9 agosto 2013, n. 98.

Capo II

Dati contenuti nel SITAM e finalità del loro trattamento

Art. 3.

Finalità dei trattamenti

1. I dati contenuti nel SITAM sono trattati a fini di controllo sulla circolazione delle armi e delle munizioni, anche nella forma del rilascio, del rinnovo o del diniego delle autorizzazioni, licenze e nulla osta previsti dalla vigente normativa, nonché a fini di prevenzione e repressione dei reati.

2. I dati contenuti nel SITAM, preventivamente resi anonimi e in forma aggregata, possono essere trattati, altresì, nell'ambito delle rispettive attribuzioni, anche per scopi statistici da:

a) gli uffici del Dipartimento della pubblica sicurezza competenti ad esercitare il controllo sulla circolazione delle armi e delle munizioni, anche nella forma del rilascio, del rinnovo o del diniego delle autorizzazioni, licenze e nulla osta previsti dalla vigente normativa, nonché in materia di prevenzione e repressione dei reati;

b) le Prefetture-UTG;

c) le Questure e gli altri uffici della Polizia di Stato, nonché i comandi e reparti dell'Arma dei carabinieri e della Guardia di finanza, competenti nella materia di cui alla lettera *a)*.

3. Per le finalità di cui al comma 2, il SITAM è dotato di un sistema per le elaborazioni statistiche che permette di analizzare in forma anonima e aggregata i dati riguardanti le armi, le parti di arma e le munizioni, nonché il numero aggregato degli armaioli, degli intermediari e degli altri soggetti che detengono le armi, le parti di arma e le munizioni.

Art. 4.

Dati contenuti nel SITAM

1. Il SITAM contiene i dati relativi alle armi, alle parti di armi da fuoco, incluse le informazioni che consentono di associarle ai rispettivi proprietari, nonché alle munizioni fabbricate, importate o introdotte nel territorio dello Stato che sono oggetto di operazioni di esportazione, di trasferimento verso Paesi dell'Unione europea ovvero di compravendita o cessione a qualunque altro titolo verso armaioli, intermediari o altri soggetti, pubblici o privati.

2. I dati relativi alle armi da fuoco e alle parti di arma da fuoco, alle armi diverse da quelle da fuoco e alle munizioni sono specificati, rispettivamente, negli Allegati A, B e C al presente regolamento. Il SITAM assicura che per ogni tipologia di operazione sia predisposta una apposita scheda informativa nella quale sono inseriti, a cura dell'operatore o dell'utente, i dati tra quelli individuati nei predetti Allegati, pertinenti alla medesima operazione, sulla base di quanto previsto dalle disposizioni di legge.

3. I dati presenti negli archivi informatici sono configurati in maniera conforme al D.P.R. 15 gennaio 2018, n. 15, e lo scambio dei dati avviene in modalità cifrata secondo metodi di comunicazione standard.

Art. 5.

Periodo di conservazione dei dati contenuti nel SITAM

1. I periodi di conservazione dei dati di cui all'articolo 4 sono stabiliti come segue:

a) per i dati di cui all'Allegato A al presente regolamento, relativi alle armi da fuoco e alle parti di arma, compresi i dati identificativi dei fornitori, degli acquirenti e dei detentori, 30 anni dalla data della distruzione dell'arma o della parte di essa;

b) per i dati di cui all'Allegato B, relativi alle armi diverse da quelle da fuoco ed alle repliche di armi antiche ad avancarica a colpo singolo, compresi i dati identificativi dei fornitori, degli acquirenti e dei detentori:

1) 30 anni dalla data della distruzione dell'arma ad aria o a gas compressi, lunga o corta, i cui proiettili erogano un'energia cinetica superiore a 7,5 joule;

2) 10 anni dalla data in cui si è conclusa l'operazione di esportazione, di trasferimento verso un Paese dell'Unione europea, ovvero di vendita o di cessione a qualunque altro titolo in favore di un soggetto diverso dagli armaioli o dagli intermediari, per l'arma da sparo a modesta capacità offensiva, funzionante ad aria o a gas compressi, i cui proiettili erogano un'energia cinetica non superiore a 7,5 joule;

c) per i dati di cui all'Allegato C, relativi alle munizioni, 5 anni dalla data in cui si è conclusa l'operazione di esportazione o importazione, di trasferimento da e verso un Paese dell'Unione europea, ovvero di vendita o di cessione a qualunque altro titolo in favore di un soggetto diverso dagli armaioli o dagli intermediari.

2. Decorsi i termini di cui al comma 1, i dati raccolti nel SITAM sono cancellati o resi anonimi con modalità automatizzate.

Art. 6.

Raffronto con i dati inseriti nel CED

1. Il SITAM, attraverso meccanismi di cooperazione applicativa, consente agli operatori di connettersi al CED, al fine di:

a) raffrontare i dati esistenti nello stesso CED, relativi alle armi e alle munizioni, con quelli acquisiti ai fini dell'immissione nel SITAM;

b) acquisire, ai fini dell'immissione nel SITAM, i dati conservati nel CED relativi alle armi, in modo da garantire la completezza ed esattezza dei dati inseriti.

Capo III

ORGANIZZAZIONE E STRUTTURA DEL SITAM

Art. 7.

Titolare del trattamento dei dati e allocazione del sistema

1. Il Dipartimento della pubblica sicurezza è il titolare del trattamento dei dati secondo quanto previsto dal decreto legislativo 18 maggio 2018, n. 51.

2. Il SITAM è istituito presso il CEN che ne garantisce la gestione tecnica e informatica, ivi compreso il profilo di sicurezza, direttamente o attraverso le Questure.

Art. 8.

Compiti del CEN

1. Per le finalità di cui all'articolo 7, il CEN è responsabile della gestione dell'infrastruttura tecnologica, della conservazione sicura dei dati e della continuità operativa del servizio anche attraverso il ripristino di emergenza delle procedure e dei dati tramite le funzioni di backup assicurate dallo stesso CEN, attraverso le proprie articolazioni.

2. Il CEN cura il ciclo di vita delle utenze degli amministratori locali SITAM presso le Questure, di cui all'articolo 10.

Art. 9.

Compiti della Direzione centrale della polizia criminale

1. La Direzione centrale della polizia criminale, attraverso la propria articolazione competente per la gestione del CED, relativamente al trattamento dei dati presenti nel SITAM, è responsabile del rilascio, secondo le politiche di sicurezza conformi agli standard stabiliti dalle vigenti normative in materia di protezione dei dati personali, dei profili di autorizzazione nei confronti di:

a) soggetti di cui all'articolo 16, comma 1, lettere *a)*, *b)*, *c)*, *d)*, *e)*, *f)* e *g)*;

b) appartenenti agli Organismi di informazione e sicurezza, di cui all'articolo 19, comma 1;

c) operatori dell'Amministrazione civile dell'interno in servizio presso le Prefetture-UTG, di cui all'articolo 18, comma 1.

2. I soggetti di cui al comma 1, lettere *a)*, *b)* e *c)* accedono al SITAM per il tramite del portale dell'articolazione competente per la gestione del CED. I soggetti di cui al comma 1, lettere *a)*, *b)* e *c)*, che accedono al portale sono identificati tramite un codice univoco e sono abilitati allo svolgimento delle funzioni applicative di competenza dell'unità organizzativa cui sono preposti o assegnati, coerentemente con l'ambito di trattamento consentito dal profilo di autorizzazione. Ai fini dell'accesso al SITAM, il codice identificativo e le credenziali di autenticazione di cui all'articolo 2, comma 3, lettera *e)*, sono conformi almeno al livello 2 di sicurezza o garanzia (Level of Assurance – LoA) previsto dallo standard internazionale ISO/IEC 29115, con impiego di un sistema di autenticazione a due fattori, non necessariamente basato su certificati digitali.

Art. 10.

Compiti delle Questure

1. Le Questure provvedono, per il tramite dell'amministratore locale SITAM, ad effettuare le seguenti operazioni:

a) abilitare, previa verifica dei requisiti previsti dal presente regolamento, gli utenti nei casi previsti dall'articolo 24;

b) verificare il corretto utilizzo delle abilitazioni per l'accesso al sistema da parte degli utenti;

c) disabilitare l'accesso al SITAM nei casi previsti dagli articoli 25 e 26.

Art. 11.

Archivi informatici del SITAM

1. Il SITAM è composto dai seguenti archivi informatici:

a) l'archivio delle armi da fuoco, nel quale sono riportati, per ciascuna arma da fuoco e per ciascuna parte di arma da fuoco, i dati di cui all'Allegato A;

b) l'archivio delle armi diverse da quelle da fuoco e delle repliche di armi antiche ad avancarica a colpo singolo, nel quale sono riportati per ciascuna arma i dati di cui all'Allegato B;

c) l'archivio delle munizioni, nel quale sono riportati per ogni unità elementare di imballaggio delle munizioni per armi da fuoco, i dati di cui all'Allegato C.

2. Gli archivi di cui al comma 1, lettere *a)* e *b)* sono strutturati in modo da consentire ai soggetti autorizzati alla consultazione di effettuare ricerche finalizzate a:

a) ricostruire la filiera dei passaggi di proprietà e comunque della cessione, a qualunque titolo, di ciascuna arma da fuoco, parte di arma da fuoco e arma diversa da quella da fuoco;

b) riepilogare le eventuali modifiche che abbiano mutato le caratteristiche tecniche dell'arma da fuoco o gli interventi di sostituzione delle parti di arma.

3. L'archivio di cui al comma 1 lettera *c)* è strutturato in modo da consentire ai soggetti autorizzati alla consultazione di effettuare ricerche finalizzate a ricostruire la filiera dei passaggi di proprietà e comunque della cessione, a qualunque titolo, di ciascuna unità elementare di imballaggio delle munizioni per armi da fuoco.

4. Gli archivi di cui al comma 1 sono, inoltre, strutturati in modo da consentire:

a) l'elaborazione automatica di un riepilogo mensile delle operazioni compiute da ciascun armaiolo e dall'intermediario e il suo invio automatico alle Questure e agli altri uffici e comandi delle Forze di polizia per le finalità previste dall'articolo 3, commi 1 e 2;

b) ai soggetti autorizzati alla consultazione, l'effettuazione di ricerche finalizzate ad acquisire i dati relativi a ciascun armaiolo, intermediario o soggetto che detenga o abbia detenuto armi, parti di arma da fuoco o munizioni;

c) la trattazione dei dati per finalità statistiche dei dati resi anonimi e aggregati, di cui all'articolo 3, commi 2 e 3.

5. L'elaborazione automatica del riepilogo mensile delle operazioni compiute dall'armaiolo o intermediario e la sua messa a disposizione delle Questure e degli altri uffici e comandi delle Forze di polizia tiene luogo della comunicazione mensile prevista dagli articoli 35, comma 4, e 55, primo comma, terzo periodo, TULPS.

Art. 12.

Collegamenti del SITAM al CED

1. Il collegamento telematico del SITAM al CED, per le finalità di cui all'articolo 6, è realizzato nel termine di cui all'articolo 34, comma 1, attraverso meccanismi di cooperazione applicativa resi disponibili dal CED, sulla base di specifici accordi inter-istituzionali.

Art. 13.

Collegamenti degli utenti al SITAM

1. Al fine di effettuare l'immissione dei dati concernenti le operazioni compiute relativamente alle armi, alle parti di arma da fuoco ed alle munizioni, nonché la consultazione e la correzione dei medesimi dati precedentemente immessi, l'armaiolo o l'intermediario richiede l'abilitazione per l'accesso al SITAM alla Questura della provincia in cui è ubicata la sede della propria impresa tenuta ad effettuare le registrazioni e comunicazioni a norma degli articoli 35 e 55 TULPS.

2. Al fine di assicurare l'inserimento, anche in forma massiva, dei dati delle armi e delle munizioni esportate, importate, fabbricate, immesse sul mercato o sulle quali sono state eseguite operazioni di carattere tecnico, l'armaiolo o l'intermediario possono utilizzare sistemi informatici gestionali, purché essi siano compatibili con le caratteristiche tecniche, informatiche e di sicurezza del SITAM e il loro collegamento al SITAM stesso non determini nuovi ed ulteriori oneri a carico della finanza pubblica.

3. Le Questure provvedono ad attivare i collegamenti tra i soggetti di cui al comma 1 e il SITAM, secondo le modalità e le procedure che sono rese note nella «*home page*» del relativo «*sito web*».

Art. 14.

Collegamenti delle Prefetture, delle Questure, delle Forze di polizia e degli Organismi di informazione e sicurezza al SITAM

1. Al fine di effettuare le operazioni di accesso, immissione ed aggiornamento previste dagli articoli 16, 17 le Questure, gli altri Uffici o Comandi delle Forze di polizia si collegano al SITAM per il tramite del CED, il quale assicura, per le finalità di cui agli articoli 18 e 19, il collegamento al SITAM delle Prefetture-UTG, del DIS, dell'AISE e dell'AISI.

Capo IV

ACCESSO, CONSULTAZIONE, IMMISSIONE E AGGIORNAMENTO DEL SITAM

Sezione I

SOGGETTI LEGITTIMATI ALL'ACCESSO, CONSULTAZIONE, IMMISSIONE ED AGGIORNAMENTO

Art. 15.

Interrogazioni del SITAM

1. Le interrogazioni del SITAM possono essere effettuate per finalità di accesso, di consultazione, di immis-

sione ed aggiornamento dei dati contenuti nello stesso SITAM; a ciascuna delle predette finalità corrisponde uno specifico profilo di autorizzazione.

2. Le interrogazioni sono effettuate dai soggetti indicati dagli articoli 16, 17, 18 e 19, ai quali siano state preventivamente rilasciate le necessarie credenziali di autenticazione.

Art. 16.

Soggetti legittimati all'accesso al SITAM

1. I soggetti che possono effettuare operazioni di accesso ai dati conservati nel SITAM sono:

a) il Questore e il dirigente che ne svolge le funzioni vicarie;

b) il personale delle Forze di polizia delle qualifiche, anche non dirigenziali, in servizio presso gli uffici del Dipartimento della pubblica sicurezza competenti ad esercitare il controllo sulla circolazione delle armi e delle munizioni, anche nella forma del rilascio, del rinnovo o del diniego delle autorizzazioni, licenze e nulla osta previsti dalla vigente normativa, nonché in materia di prevenzione e repressione dei reati;

c) il personale della Polizia di Stato, anche delle qualifiche non dirigenziali, della Questura e degli uffici di pubblica sicurezza, preposto o addetto agli uffici, competenti ad esercitare il controllo sulla circolazione delle armi e delle munizioni, anche nella forma del rilascio, del rinnovo o del diniego delle autorizzazioni, licenze e nulla osta previsti dalla vigente normativa, nonché in materia di prevenzione e repressione dei reati;

d) gli ufficiali dell'Arma dei carabinieri e della Guardia di finanza preposti o addetti a comandi, unità o reparti, competenti a contribuire, anche sul piano informativo, alle attività di controllo sulla circolazione delle armi e delle munizioni, nonché in materia di prevenzione e repressione dei reati;

e) il personale dell'Arma dei carabinieri e della Guardia di finanza appartenente ai comandi, unità o reparti di cui alla lettera *d)*, autorizzato dai relativi responsabili;

f) il personale dell'Amministrazione civile dell'interno delle qualifiche non dirigenziali, addetto alle articolazioni della Questura, nonché degli altri uffici locali di pubblica sicurezza, competenti ad esercitare il controllo sulla circolazione delle armi e delle munizioni, anche nella forma del rilascio, del rinnovo o del diniego delle autorizzazioni, licenze e nulla osta previsti dalla vigente normativa;

g) il personale dell'Amministrazione civile dell'interno delle qualifiche non dirigenziali, addetto alle articolazioni del Dipartimento della pubblica sicurezza, competenti ad esercitare il controllo sulla circolazione delle armi e delle munizioni, anche nella forma del rilascio, del rinnovo o del diniego delle autorizzazioni, licenze e nulla osta previsti dalla vigente normativa.

2. Le operazioni di accesso ai dati conservati nel SITAM possono altresì essere effettuate dall'amministratore locale SITAM limitatamente allo svolgimento delle attività, di sicurezza, tenuta e conservazione dei dati.

3. L'accesso da parte dei soggetti di cui ai commi 1 e 2 avviene esclusivamente per il tramite del portale di accesso ai servizi dell'articolazione competente per la gestione del CED, mediante tecniche di identità federata, con accreditamento unico per l'intero dominio, secondo le politiche di sicurezza conformi agli standard stabiliti dalle vigenti normative in materia di protezione dei dati personali.

Art. 17.

Soggetti legittimati all'immissione e all'aggiornamento dei dati contenuti nel SITAM

1. L'immissione e l'aggiornamento di dati nel SITAM sono eseguiti esclusivamente dal personale di cui all'articolo 16, commi 1 e 2, preventivamente autorizzato dal Questore ovvero dal responsabile del competente ufficio o comando di livello provinciale delle Forze di polizia.

2. Gli utenti possono essere abilitati ad effettuare operazioni di immissione e aggiornamento finalizzate esclusivamente ad inserire nel SITAM i dati indicati negli Allegati A, B, C necessari per assolvere agli obblighi di registrazione e comunicazione di cui agli articoli 35 e 55 TULPS. Per le finalità di cui al presente comma, gli utenti possono eseguire operazioni di consultazione, limitatamente ai dati da essi precedentemente immessi nel SITAM.

3. Per le finalità di cui all'articolo 13, comma 1, l'armaiolo o l'intermediario utilizzano la propria identità digitale, anche ad uso professionale, attraverso lo SPID di livello 3, ovvero la CIE, ovvero un regime di identificazione elettronica notificato da uno Stato membro di livello di garanzia elevato, ai sensi degli articoli 8 e 9 del Regolamento UE 910/2014.

4. L'armaiolo o l'intermediario che non ha l'abilitazione per l'accesso al SITAM in quanto titolare di un regime di identificazione elettronica non ancora notificato dallo Stato membro ai sensi dell'articolo 9 del Regolamento UE 910/2014, continua a tenere il registro delle operazioni giornaliere di cui agli articoli 35 e 55 TULPS e adempie alla comunicazione mensile prevista dai medesimi articoli 35 e 55 TULPS su supporto informatico sottoscritto con firma qualificata secondo le modalità indicate nella «*home page*» del relativo «*sito web*».

5. Gli amministratori locali SITAM presso le Questure, verificati i requisiti previsti, provvedono ad abilitare le utenze di accesso al SITAM per i soggetti di cui al comma 2.

6. Il SITAM è dotato di funzionalità che consentono la correzione di eventuali errori materiali commessi nell'immissione dei dati.

7. Gli operatori, gli operatori dell'Amministrazione civile dell'interno in servizio presso le Questure effettuano tempestivamente la correzione degli eventuali errori materiali.

8. Gli utenti effettuano la correzione per via telematica degli eventuali errori materiali commessi, entro settantadue ore lavorative dalla prima immissione degli stessi. Decorso tale termine, gli utenti comunicano l'errore materiale commesso e la correzione da apportare alla Questura territorialmente competente, che provvede all'immissione, dopo aver verificato l'esattezza delle relative correzioni.

Art. 18.

Consultazione del SITAM da parte del personale dell'Amministrazione civile dell'interno in servizio presso le Prefetture-UTG

1. Il SITAM può essere consultato dal seguente personale appartenente all'Amministrazione civile dell'interno:

a) Prefetti in servizio presso le Prefetture-UTG;

b) viceprefetti vicari delle Prefetture-UTG;

c) personale, anche delle carriere non dirigenziali, preposto o addetto agli uffici della Prefettura-UTG, competenti ad esercitare il controllo sulla circolazione delle armi e delle munizioni, anche nella forma del rilascio, del rinnovo o del diniego delle autorizzazioni, licenze e nulla osta previsti dalla vigente normativa.

2. Al predetto personale sono rilasciate, dall'articolazione competente per la gestione del CED, le credenziali di autenticazione che consentono esclusivamente le operazioni di consultazione del SITAM.

Art. 19.

Consultazione del SITAM da parte degli appartenenti agli Organismi di informazione e sicurezza

1. In attuazione di quanto previsto dall'articolo 13, comma 2, della legge 3 agosto 2007, n. 124 e dal relativo regolamento di attuazione, al personale del DIS, dell'AISE e dell'AISI sono rilasciate, dall'articolazione competente per la gestione del CED, le credenziali di autenticazione che consentono unicamente l'effettuazione di operazioni di consultazione del SITAM.

Art. 20.

Tracciabilità delle operazioni compiute sul SITAM

1. Le interrogazioni e le correzioni di errori materiali effettuati dagli operatori, dagli operatori dell'Amministrazione civile dell'interno e dagli utenti autorizzati sono registrati in appositi file di log, non modificabili, che sono conservati per 20 anni dall'accesso o dall'operazione.

2. Le registrazioni delle operazioni di cui al comma 1 consentono di conoscere i motivi, la data e l'ora di tali operazioni e identificare la persona che ha eseguito le operazioni e i destinatari.

3. L'accesso alle registrazioni di cui al comma 1 è consentito solamente ai fini della verifica della liceità del trattamento, del controllo interno, per garantire l'integrità e la sicurezza dei dati personali e nell'ambito del procedimento penale, da parte del responsabile per la protezione dei dati della Polizia di Stato, di cui all'articolo 10, comma 3, del decreto del Ministro dell'interno 6 febbraio 2020 e dai dirigenti degli Uffici e Comandi di cui all'articolo 22, comma 1.

Sezione II

Caratteristiche e rilascio delle credenziali di autenticazione

Art. 21.

Credenziali di autenticazione

1. Per l'effettuazione di operazioni di accesso, di immissione, di aggiornamento e di consultazione dei dati, i soggetti legittimati devono preventivamente munirsi delle credenziali di autenticazione per eseguire la connessione in sicurezza al SITAM.

2. Le credenziali di autenticazione sono individuali e non sono cedibili; ad esse è associato il profilo di autorizzazione della categoria di soggetti legittimati.

3. Le credenziali di autenticazione non possono essere utilizzate per l'esecuzione di operazioni diverse da quelle previste dal profilo di autorizzazione per cui sono rilasciate.

4. Le credenziali di autenticazione rilasciate al personale del CEN possono essere utilizzate esclusivamente per lo svolgimento delle attività relative alla gestione dell'infrastruttura tecnologica, di sicurezza, tenuta e conservazione dei dati, di cui all'articolo 8.

5. Le credenziali rilasciate agli amministratori locali SITAM presso le Questure sono utilizzate per le attività di cui all'articolo 17, comma 5.

Art. 22.

Assegnazione delle credenziali di autenticazione al personale in servizio presso gli uffici e comandi delle Forze di polizia, per finalità di accesso, di immissione o di aggiornamento dei dati

1. Il Questore o, su sua delega, il dirigente che ne svolge le funzioni vicarie, e il responsabile del competente ufficio o comando di livello provinciale delle Forze di polizia comunicano, per via telematica, all'articolazione competente per la gestione del CED, gli elenchi dei propri dipendenti per i quali viene richiesto il rilascio delle credenziali di autenticazione per finalità di accesso, di immissione o aggiornamento dei dati.

2. Per ciascun operatore devono essere riportati i seguenti dati:

a) nome e cognome;

b) data e luogo di nascita;

c) luogo di residenza;

d) codice fiscale;

e) qualifica o grado;

f) Ufficio di appartenenza;

g) casella di posta elettronica assegnata dall'Amministrazione.

3. L'articolazione competente per la gestione del CED genera le credenziali di autenticazione e le assegna individualmente a ciascuno dei soggetti di cui all'articolo 9, secondo le politiche di sicurezza adottate.

4. La procedura di cui al comma 1 si applica anche al personale non dirigente della Amministrazione civile dell'interno, preposto o addetto agli uffici della Questura competenti ad esercitare il controllo sulla circolazione delle armi e delle munizioni, anche nella forma del rilascio, del rinnovo o del diniego delle autorizzazioni, licenze e nulla osta previsti dalla vigente normativa.

Art. 23.

Assegnazione delle credenziali di autenticazione al personale dell'Amministrazione civile dell'interno in servizio presso le Prefetture-UTG per finalità di consultazione

1. L'assegnazione delle credenziali di autenticazione per finalità di consultazione in favore del personale dell'Amministrazione civile dell'interno di cui all'articolo 18 è richiesto dal Prefetto o, su sua delega, dal viceprefetto vicario all'articolazione competente per la gestione del CED.

Art. 24.

Richiesta di abilitazione degli utenti per finalità di accesso, di immissione o di aggiornamento dei dati

1. L'armaiolo, il suo rappresentante, ovvero l'intermediario, titolare di un'identità digitale di cui all'articolo 17, comma 3, richiede l'abilitazione per l'accesso al SITAM alla Questura:

a) del luogo in cui ha sede legale l'impresa, relativamente all'armaiolo o all'intermediario;

b) del luogo in cui si trova lo stabilimento, l'opificio o il ramo d'azienda per la cui gestione il rappresentante dell'armaiolo ha conseguito l'approvazione ai sensi dell'articolo 8, secondo comma, TULPS;

c) del luogo in cui si trova lo stabilimento, l'opificio o la sede dell'impresa presso i quali i dipendenti dell'armaiolo e dell'intermediario svolgono la propria attività lavorativa.

2. La Questura provvede a verificare che il soggetto che ha richiesto l'abilitazione per l'accesso al SITAM rivesta la qualità di utente e comunica l'avvenuta abilitazione.

3. Fuori dai casi di cui agli articoli 10 e 11, terzo comma, TULPS, la Questura può denegare l'abilitazione per l'accesso al SITAM nel caso in cui accerti che la persona per la quale essa viene richiesto non possiede i requisiti stabiliti dall'articolo 11 TULPS, primo e secondo comma del medesimo.

4. L'abilitazione per l'accesso al SITAM è revocata nel caso in cui sia stato negato, con provvedimento espresso, il rinnovo della licenza relativa all'attività in materia di armi e munizioni ovvero nel caso in cui in cui la medesima licenza sia stata revocata. Nel caso in cui la predetta licenza sia stata sospesa, anche l'abilitazione per l'accesso al SITAM è sospesa per un periodo di pari durata. Nelle more del rinnovo della licenza relativa all'attività in materia di armi e munizioni, l'abilitazione per l'accesso al SITAM continua ad essere attiva.

5. L'armaiolo o l'intermediario possono eseguire le operazioni di immissione, di aggiornamento e di correzione dei dati al solo fine di assolvere agli obblighi di registrazione e comunicazione previsti dagli articoli 35 e 55 TULPS. Il rappresentante può eseguire le predette operazioni esclusivamente per assolvere agli obblighi di registrazione delle operazioni effettuate nello stabilimento, opificio o nella sede dell'impresa per la cui gestione ha ottenuto l'approvazione ai sensi dell'articolo 8, secondo comma, TULPS. I dipendenti dell'armaiolo e dell'intermediario possono eseguire le predette operazioni esclusivamente per assolvere agli obblighi di registrazione delle operazioni effettuate nello stabilimento, opificio o nella sede dell'impresa, presso i quali svolgono la loro attività lavorativa.

6. Salvo quanto previsto dall'articolo 26 o da altre disposizioni di legge, la Questura territorialmente competente provvede a disabilitare l'accesso al SITAM nel caso in cui siano state effettuate operazioni di immissione, di aggiornamento e di correzione per finalità diverse da quelle di cui all'articolo 17, comma 2.

Art. 25.

Validità dell'abilitazione per l'accesso al SITAM e delle credenziali di autenticazione

1. L'abilitazione per l'accesso al SITAM rilasciata agli utenti è valida per il periodo di validità della licenza sulla base della quale l'armaiolo o l'intermediario opera. Decorso tale periodo ne deve essere richiesto il rinnovo secondo la procedura stabilita dall'articolo 24.

2. Le credenziali di autenticazione rilasciate ai soggetti di cui all'articolo 16, comma 1, sono valide per il periodo di tempo previsto dalle politiche di sicurezza stabilite per il CED.

3. I soggetti di cui agli articoli 16, comma 1, e 18, comma 1, nel caso di trasferimento ad altro incarico o di cessazione e sospensione del rapporto di lavoro dipendente, danno immediata comunicazione all'articolazione competente per la gestione del CED.

4. I soggetti di cui all'articolo 17, comma 2, nel caso di loro trasferimento ad altro incarico o di cessazione e sospensione del rapporto di lavoro, danno immediata comunicazione alla Questura territorialmente competente.

5. I soggetti di cui all'articolo 22, comma 1, disabilitano, attraverso anche il Focal Point, le credenziali di autenticazione degli amministratori locali SITAM trasferiti ad altro incarico o il cui rapporto di dipendenza sia cessato o sospeso.

6. Le credenziali di autenticazione non utilizzate da almeno dodici mesi sono disabilitate automaticamente. Le credenziali del personale del CEN e degli amministratori locali delle Questure sono valide per il periodo di tempo previsto dalle politiche di sicurezza stabilite dall'Amministrazione.

Art. 26.

Uso delle credenziali

1. I soggetti di cui all'articolo 2, comma 2, lettere *g)* e *h)*, che hanno ottenuto le credenziali di autenticazione al SITAM di cui agli articoli 22 e 23 effettuano il primo accesso secondo le politiche di sicurezza stabilite per il CED.

2. Le credenziali di autenticazione di cui al comma 1 sono personali e il loro utilizzo è consentito esclusivamente ai titolari per le finalità di cui al presente regolamento.

3. I titolari delle credenziali di cui al comma 1 sono tenuti a custodire le credenziali di autenticazione in modo da evitare che terzi possano appropriarsene o farne utilizzo.

4. L'abilitazione al SITAM rilasciata agli utenti è personale e consente l'accesso solo ai titolari per le finalità di cui al presente regolamento.

5. I titolari delle credenziali di autenticazione sono tenuti a comunicare immediatamente all'articolazione competente per la gestione del CED e al proprio superiore in linea disciplinare lo smarrimento o il furto delle credenziali di autenticazione. Il furto o lo smarrimento dell'identità digitale, utilizzata per l'accesso al SITAM, sono comunicati immediatamente alla Questura territorialmente competente che provvede alla disabilitazione dell'accesso.

6. L'uso improprio dell'abilitazione per l'accesso al SITAM da parte dell'armaiolo è valutato ai sensi dell'articolo 10 TULPS e ne è fatto rapporto all'autorità giudiziaria per la valutazione degli eventuali profili di rilevanza penale.

7. L'uso improprio dell'abilitazione da parte dei dipendenti dell'armaiolo e delle credenziali per l'accesso al SITAM da parte dei soggetti di cui al comma 1 comporta la revoca immediata dell'abilitazione stessa che può essere ripristinata trascorsi dodici mesi, in presenza dei necessari requisiti.

Capo V

Immissione ed aggiornamento dei dati inseriti nel SITAM

Art. 27.

Immissione di dati ai fini di assolvimento degli obblighi di registrazione di cui agli articoli 35 e 55 TULPS

1. Al fine di adempiere agli obblighi di registrazione e comunicazione di cui agli articoli 35 e 55 TULPS, gli utenti immettono nel SITAM i dati indicati negli Allegati A, B, C per ciascuna operazione compiuta riguardante, rispettivamente, le armi da fuoco e le parti di arma, le armi diverse da quelle da fuoco, le repliche di armi antiche ad avancarica a colpo singolo, le munizioni. L'immissione dei dati è eseguita giornalmente secondo l'ordine cronologico di effettuazione di ciascuna operazione.

2. Il SITAM implementa apposite funzioni, al fine di consentire agli utenti di eseguire, entro settantadue ore, per via telematica, correzioni o rettifiche di eventuali errori materiali compiuti nelle operazioni di immissione dei dati, ai sensi e per gli effetti di cui all'articolo 17, commi 6, 7 e 8. Il SITAM conserva la registrazione in ordine cronologico delle correzioni e delle rettifiche apportate dagli utenti, garantendo l'identificazione del soggetto che le ha effettuate.

3. Il SITAM segnala, in un apposito registro accessibile alle Questure e agli altri uffici e comandi delle Forze di polizia, le correzioni o le rettifiche dei dati inseriti, apportate ai sensi del comma 2.

Art. 28.

Immissione ed aggiornamento dei dati da parte delle Questure e degli altri uffici e comandi delle Forze di polizia

1. Le Questure, gli uffici di pubblica sicurezza, i comandi territoriali dell'Arma dei carabinieri immettono nel SITAM i dati indicati negli Allegati A, B, C riguardanti le seguenti operazioni compiute da soggetti privati diversi dall'armaiolo o dall'intermediario aventi ad oggetto armi da fuoco, parti di arma, armi diverse da quelle da fuoco ovvero le repliche di armi antiche ad avancarica a colpo singolo:

a) denuncia di detenzione di arma da fuoco o di parte di arma;

b) cessione o acquisto dell'arma da fuoco o di parte di arma;

c) furto, appropriazione indebita, smarrimento e rinvenimento dell'arma da fuoco o di parte di arma;

d) ritiro cautelare e confisca dell'arma da fuoco o di parte di arma disposto, ai sensi delle vigenti normative, dall'Autorità provinciale di pubblica sicurezza;

e) disattivazione o distruzione dell'arma da fuoco;

f) versamento spontaneo dell'arma da fuoco presso la Questura ovvero presso gli altri uffici e comandi delle Forze di polizia.

2. Le Questure, gli uffici di pubblica sicurezza, i comandi territoriali dell'Arma dei carabinieri immettono nel SITAM i dati indicati negli Allegati A, B, C riguardanti le seguenti operazioni aventi ad oggetto munizioni nel caso in cui esse siano compiute da soggetti privati diversi dall'armaiolo o dall'intermediario e siano assoggettate all'obbligo di denuncia o di licenza rilasciata dall'Autorità di pubblica sicurezza:

a) denuncia di detenzione di munizioni;

b) cessione o acquisto di munizioni;

c) furto o smarrimento di munizioni;

d) ritiro cautelare e confisca delle munizioni disposto, ai sensi delle vigenti normative, dall'Autorità provinciale di pubblica sicurezza;

e) distruzione delle munizioni;

f) versamento spontaneo delle munizioni presso la Questura ovvero presso gli altri uffici e comandi delle Forze di polizia.

3. Gli uffici e comandi delle Forze di polizia provvedono, inoltre, ad immettere nel SITAM i dati relativi alle armi da fuoco, alle parti di arma, alle armi diverse da quelle da fuoco, alle repliche di armi antiche ad avancarica a colpo singolo e alle munizioni di cui l'Autorità giudiziaria abbia disposto il sequestro o la confisca nell'ambito di procedimenti penali o di procedimenti per l'applicazione di una misura di prevenzione personale o patrimoniale.

4. Le Questure, gli uffici di pubblica sicurezza e gli altri uffici e comandi delle Forze di polizia effettuano le immissioni di dati di cui al presente articolo giornalmente e, comunque senza ritardo, secondo l'ordine cronologico di svolgimento di ciascuna operazione.

5. Per le finalità di cui al presente articolo, il SITAM e il CED dialogano attraverso meccanismi di cooperazione applicativa che consentono anche di semplificare le operazioni di immissione e aggiornamento dei dati.

Art. 29.

Immissione dei dati riguardanti le armi conservate presso i musei

1. I direttori dei musei di Stato e altri istituti della cultura di cui all'articolo 101 del decreto legislativo 22 gennaio 2004, n. 42, di altri enti pubblici o appartenenti a enti morali, cui è affidata la custodia e la conservazione di raccolte di armi da guerra o tipo guerra, di munizioni da guerra, di collezioni di armi comuni da sparo, di collezioni di armi artistiche, rare o antiche, comunicano immediatamente i dati relativi ai predetti materiali iscritti nell'inventario previsto dall'articolo 32, primo comma, della legge n. 110 del 1975 ed i loro aggiornamenti alla Questura territorialmente competente che provvede ad immetterli nel SITAM, secondo le modalità previste dall'articolo 28.

Art. 30.

Controllo sulle operazioni di accesso, consultazione, immissione e aggiornamento dei dati

1. I responsabili degli uffici e dei comandi di cui all'articolo 16, comma 1, verificano periodicamente che le interrogazioni del SITAM siano effettuate per le finalità previste dal presente regolamento.

2. Nei confronti del personale in servizio presso le Prefetture-UTG e presso le Questure il controllo è esercitato, rispettivamente, dal viceprefetto vicario e dal dirigente che svolge le funzioni vicarie del Questore.

3. La Questura può sempre richiedere informazioni agli utenti, al fine di accertare la correttezza delle operazioni di trattamento dei dati effettuati. A tale scopo, la Questura può utilizzare i riepiloghi mensili di cui all'articolo 11, comma 4, lettera *a)*.

Art. 31.

Adempimenti nel caso di mancato funzionamento del SITAM

1. Nel caso in cui il SITAM non sia in grado di funzionare regolarmente a causa di eventi eccezionali, i soggetti di cui all'articolo 2, comma 2, lettere *g)*, *h)*, limitatamente agli operatori dell'Amministrazione civile dell'interno in servizio presso le Questure, ed *i)*, effettuano le registrazioni dei dati previste dal presente regolamento su supporti cartacei ovvero su supporti informatici conformi agli standard di sicurezza stabiliti dalle vigenti norme in materia di protezione dei dati personali.

2. Al fine di salvaguardare la possibilità di effettuare i controlli di pubblica sicurezza, gli armaioli e gli intermediari trasmettono, anche per via telematica, alla Questura competente per territorio, i dati registrati sui supporti provvisori entro il giorno successivo a quello cui le registrazioni si riferiscono.

3. Successivamente al ripristino della regolare funzionalità, i soggetti di cui al comma 1 provvedono ad inserire tempestivamente nel SITAM i dati registrati sui supporti provvisori, anche al fine di adempiere agli obblighi di cui agli articoli 35 e 55 TULPS.

Art. 32.

Violazione dei dati personali

1. In caso di violazione dei dati personali si applica l'articolo 26 del decreto legislativo n. 51 del 2018.

Art. 33.

Scambio d'informazioni con gli Stati membri dell'Unione europea e con Stati terzi

1. In caso di trasferimento definitivo di un'arma da fuoco verso uno Stato membro, le pertinenti informazioni raccolte nel SITAM sono comunicate a tale Stato per il tramite dell'autorità nazionale, previa verifica della loro esattezza, aggiornamento e completezza. In caso di trasferimento definitivo di un'arma da fuoco da uno Stato membro verso il territorio nazionale, le informazioni sono ricevute dall'autorità nazionale, la quale provvede all'inserimento nel SITAM.

2. La comunicazione e la ricezione delle informazioni di cui al comma 1 avviene in modalità elettronica, utilizzando il sistema di informazione del mercato interno («IMI») tra le autorità competenti, in conformità a quanto previsto dal regolamento delegato (UE) 2019/686.

3. Nel caso di esportazione o importazione a titolo definitivo verso o da uno Stato terzo, lo scambio delle pertinenti informazioni è consentito in conformità agli accordi o alle intese sottoscritte e rese esecutive con tali Stati, qualora non in contrasto con gli atti normativi interni o dell'Unione europea. La comunicazione può anche avvenire per via telematica, assicurando l'adozione di misure adeguate per garantire la riservatezza e l'integrità delle informazioni trasmesse.

Capo VI

Norme finali e transitorie

Art. 34.

Entrata in funzione del SITAM

1. Il Dipartimento della pubblica sicurezza provvede ad ultimare il SITAM entro diciotto mesi dalla data di entrata in vigore del presente regolamento. Entro e non oltre i successivi tre mesi il predetto Dipartimento assicura che siano completate le attività organizzative e propedeutiche, ivi comprese quelle riguardanti l'assegnazione delle credenziali di autenticazione ai soggetti di cui agli articoli 22 e 23, necessarie per la messa in funzione del SITAM e che il CED renda disponibili al SITAM stesso i dati relativi alle armi e alle parti di arma di cui all'articolo 28, commi 1 e 3, al fine di garantire la migliore funzionalità del sistema.

2. Il Dipartimento della pubblica sicurezza rende noto il completamento delle attività di cui al comma 1 mediante pubblicazione di un apposito avviso sul proprio sito istituzionale.

3. A decorrere dalla data di pubblicazione dell'avviso di cui al comma 2, gli utenti possono presentare alla Questura le richieste di primo rilascio dell'abilitazione per l'accesso al SITAM ai sensi dell'articolo 24.

4. Il SITAM è reso operativo decorsi ventiquattro mesi dalla data di entrata in vigore del presente regolamento.

5. Le disposizioni di cui al Capo V trovano applicazione a decorrere dal termine previsto dal comma 4.

Art. 35.

Oneri informativi introdotti

1. Gli oneri informativi introdotti dal presente regolamento, ai sensi dell'articolo 7 della legge 11 novembre 2011, n. 180, sono indicati nell'Allegato D.

Art. 36.

Clausola di invarianza finanziaria

1. Dall'attuazione del presente regolamento non devono derivare nuovi o maggiori oneri a carico dello Stato. L'Amministrazione della pubblica sicurezza provvede all'espletamento dei compiti ad essa attribuiti dal presente regolamento con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente, anche in conformità a quanto stabilito dall'articolo 11, comma 7, del decreto legislativo 10 agosto 2018, n. 104, in ordine agli stanziamenti previsti per le attività di gestione e manutenzione del sistema.

Il presente decreto sarà trasmesso alla Corte dei conti per la registrazione.

Il presente decreto, munito del sigillo dello Stato, sarà inserito nella Raccolta ufficiale degli atti normativi della Repubblica italiana. È fatto obbligo a chiunque spetti di osservarlo e farlo osservare.

Roma, 12 luglio 2023

Il Ministro dell'interno
PIANTEDOSI

Il Ministro dell'economica e delle finanze
GIORGETTI

Visto, *il Guadasigilli:* NORDIO

Registrato alla Corte dei conti il 3 agosto 2023

Ufficio di controllo sugli atti del Ministero dell'interno e del Ministero della difesa, reg.ne n. 2803

ALLEGATO *A*

art. 4, comma 2

DATI RELATIVI ALLE ARMI DA FUOCO E ALLE PARTI D'ARMA DA FUOCO

1. Per le armi da fuoco insieme alle sue parti, il SITAM contiene i seguenti dati inseriti in appositi campi identificativi:

a) fabbricante o assemblatore (codice fiscale, partita Iva o ragione sociale);

b) Paese o il luogo di fabbricazione o assemblaggio;

c) numero di serie;

d) anno di fabbricazione o assemblaggio;

e) tipo (ad esempio carabina, fucile, pistola, …);

f) marca;

g) modello, ove presente;

h) calibro;

i) marcatura applicata alle relative parti nel caso in cui questa differisca dalla marcatura unica applicata sul telaio o sul fusto dell'arma stessa. Qualora la parte dell'arma sia di dimensioni troppo ridotte per essere provvista della marcatura, essa è contrassegnata almeno da un numero di serie o da un codice alfanumerico digitale, che troverà collocazione nel presente campo;

l) codice identificativo corrispondente alla classificazione effettuata dal Banco Nazionale di Prova;

m) classificazione dell'arma nella categoria europea effettuata dal Banco Nazionale di Prova (ivi compreso il cambiamento, a seguito di interventi tecnici, della categoria o della sottocategoria dell'arma da fuoco di cui all'Allegato I alla direttiva 91/477/CEE);

n) dati identificativi dell'operatore economico o privato che cede l'arma (cedente, comodante, esportatore, riparatore, venditore, ecc.);

o) dati identificativi dell'operatore economico o privato che acquisisce l'arma (acquirente, cessionario, comodatario, importatore, riparatore, ecc..);

p) dati identificativi del detentore e luogo di detenzione;

q) operazioni aventi ad oggetto l'arma e la data in cui le stesse sono state effettuate (quali ad esempio: cessione, acquisto, acquisto per successione, acquisto per ritrovamento, cambio luogo detenzione, comodato, trasferimento intracomunitario, demilitarizzazione, disattivazione, esportazione, importazione, riparazione, vendita, rottamazione, ecc.);

r) prezzo dell'arma (il dato deve essere inserito dagli operatori economici, ex articolo 54 R.D. 6 maggio 1940, n. 635);

s) estremi del titolo abilitativo esibito per l'acquisto dell'arma (nulla osta all'acquisto di armi; licenza di porto d'armi; licenza ex articolo 31 TULPS, collezione di armi antiche ex D.M. 28 aprile 1982, ecc.);

t) estremi della licenza o autorizzazione nell'ipotesi di esportazione, importazione o trasferimento intracomunitario (indicare la denominazione del titolo autorizzatorio, l'autorità che lo ha emesso e la data del rilascio);

u) eventuali ulteriori dati facoltativi.

2. Per le armi da fuoco antiche, l'inserimento è limitato ai dati conosciuti o comunque rilevabili dalla denuncia o da qualunque altra certificazione o documentazione presentata dall'interessato, ai sensi dell'articolo 38 TULPS.

3. I dati di cui alle lettere da *a)* ad *h)* costituiscono gli elementi della marcatura unica (di cui all'articolo 11, primo comma, della legge n. 110 del 1975).

———

ALLEGATO *B*

art. 4, comma 2

DATI RELATIVI ALLE ARMI DIVERSE DA QUELLE DA FUOCO ED ALLE REPLICHE DI ARMI ANTICHE AD AVANCARICA A COLPO SINGOLO

1. Per le armi diverse da quelle da fuoco il SITAM contiene i seguenti dati inseriti in appositi campi identificativi:

a) fabbricante o assemblatore (codice fiscale o partita Iva, ragione sociale);

b) Paese o il luogo di fabbricazione o assemblaggio;

c) numero di serie;

d) anno di fabbricazione o assemblaggio;

e) tipo (ad esempio carabina, fucile, lancia siringhe, pistola, …);

f) marca;

g) modello, ove presente;

h) calibro;

i) numero di verifica di conformità (nell'ipotesi di arma da sparo a modesta capacità offensiva, funzionante ad aria o a gas compressi, i cui proiettili erogano un'energia cinetica non superiore a 7,5 joule);

l) dati identificativi dell'operatore economico o privato che cede l'arma (cedente, comodante, esportatore, riparatore, venditore, ecc.);

m) dati identificativi dell'operatore economico o privato che acquisisce l'arma (acquirente, cessionario, comodatario, importatore, riparatore, ecc.); tale dato è richiesto per il privato solo nel caso di acquisto da operatore economico;

n) dati identificativi del detentore e luogo di detenzione (nell'ipotesi di arma da sparo, funzionante ad aria o a gas compressi, i cui proiettili erogano un'energia cinetica superiore a 7,5 joule);

o) operazioni aventi ad oggetto l'arma e la data in cui sono state effettuate (quali ad esempio: acquisto, acquisto per successione, acquisto per ritrovamento, cambio luogo detenzione, comodato, trasferimento intracomunitario, demilitarizzazione, disattivazione, esportazione, importazione, riparazione, vendita, ecc.);

p) prezzo dell'arma (il dato deve essere inserito dagli operatori economici, ex articolo 54 R.D. 6 maggio 1940, n. 635);

q) estremi del titolo abilitativo esibito per l'acquisto dell'arma (o del documento di riconoscimento dell'acquirente maggiorenne qualora trattasi di arma da sparo a modesta capacità offensiva, funzionante ad aria o a gas compressi, i cui proiettili erogano un'energia cinetica non superiore a 7,5 joule o di replica di arma antica ad avancarica a colpo singolo);

r) codice identificativo corrispondente alla classificazione effettuata dal Banco Nazionale di Prova, (nell'ipotesi di arma da sparo, funzionante ad aria o a gas compressi, i cui proiettili erogano un'energia cinetica superiore a 7,5 joule);

s) eventuali ulteriori dati facoltativi.

———

ALLEGATO *C*

art. 4, comma 2

DATI RELATIVI ALLE MUNIZIONI

1. Per le munizioni, il SITAM contiene i seguenti dati inseriti in appositi campi identificativi:

a) produttore ovvero colui per il quale, ai sensi dell'articolo 3, comma 2, della legge 6 dicembre 1993, n. 509, le munizioni sono state caricate e che ne assume la garanzia di conformità alle prescrizioni (codice fiscale o partita Iva, ragione sociale);

b) denominazione commerciale o la denominazione secondo le norme;

c) numero di identificazione del lotto delle munizioni oggetto dell'operazione;

d) quantità di confezioni delle munizioni oggetto dell'operazione;

e) quantità di cartucce contenute nell'unità elementare di imballaggio;

f) calibro;

g) tipo (palla in piombo, palla in ottone, ecc.);

h) luogo di fabbricazione;

i) dati identificativi dell'operatore economico o privato che cede le munizioni (cedente, esportatore, venditore, ecc.);

l) dati identificativi dell'operatore economico o privato che acquisisce le munizioni (acquirente, cessionario, importatore, ecc.);

m) dati identificativi del detentore e luogo di detenzione;

n) estremi del titolo abilitativo esibito per l'acquisto (nulla osta all'acquisto di munizioni; licenza di porto d'armi; licenza ex articolo 47 TULPS);

o) operazioni aventi ad oggetto le munizioni e la data in cui sono state effettuate (quali ad esempio: acquisto, acquisto per ritrovamento, cambio luogo detenzione, comodato, trasferimento intracomunitario, esportazione, importazione, vendita, ecc.);

p) eventuali ulteriori dati facoltativi.

ALLEGATO *D*

art. 35

ELENCO DEGLI ONERI INFORMATIVI INTRODOTTI A CARICO DI CITTADINI E IMPRESE

ONERI ELIMINATI

I) Denominazione

Obbligo di tenuta e di compilazione del registro su supporto cartaceo ex articoli 35 e 55 TULPS delle operazioni giornaliere aventi ad oggetto le armi e le munizioni.

Riferimento normativo interno

Articolo 11, comma 3, decreto legislativo 10 agosto 2018, n. 104

Articolo 24, comma 5, dell'intervento regolatorio

Comunicazione o dichiarazione	Domanda	Documentazione da conservare	Altro
		X	

Cosa cambia per il cittadino e/o impresa

Gli articoli 35 e 55 TULPS prevedono che i soggetti, titolari delle necessarie licenze di polizia per l'esercizio di attività di impresa o professionali in materia di armi e munizioni (d'ora in poi indicati come: «armaioli»), nonché gli intermediari ex articolo 31-*bis* TULPS (d'ora in poi indicati come: «intermediari»), sono obbligati a tenere e conservare appositi registri sui quali devono annotare le «operazioni» giornaliere aventi ad oggetto i predetti materiali.

Non essendo stata ancora compiutamente attuata la previsione di cui all'articolo 16, terzo comma, del Regolamento di esecuzione del predetto TULPS sulla tenuta informatica dei registri di polizia, gli operatori in discorso hanno conservato i registri delle operazioni in tema di armi e munizioni su supporto cartaceo.

L'articolo 11 del decreto legislativo n. 104/2018 punta a superare definitivamente questa situazione.

La disposizione, nel prevedere l'istituzione presso il Dipartimento della pubblica sicurezza di un sistema informatico per la tracciabilità delle armi e delle munizioni (SITAM), stabilisce che i cennati operatori economici e professionali immettano i dati relativi alle attività svolte nella «piattaforma» e che tale adempimento venga a sostituire l'obbligo di tenuta e compilazione del registro cartaceo (articolo 11, comma 3, del decreto legislativo n. 104/2018).

Questa soluzione viene ad essere attuata nel dettaglio dal presente intervento regolatorio che, in particolare agli articoli 13 e 24, consente che gli operatori economici e professionali assolvano agli obblighi di registrazione prescritti dagli articoli 35 e 55 TULPS, attraverso l'immissione dei pertinenti dati nel SITAM.

In tal modo, viene sancito il definitivo superamento dell'obbligo di tenuta del registro cartaceo e la sua sostituzione con il semplice inserimento dei pertinenti dati in una «*repository*» attestata e gestita dalle competenti «strutture» dell'Amministrazione della pubblica sicurezza.

II) Denominazione

Obbligo di comunicare ogni mese alla Questura territorialmente competente le generalità dei soggetti che hanno acquistato armi o munizioni (articoli 35, comma 4, e 55, primo comma, TULPS).

Riferimento normativo interno

Articolo 11, comma 5, dell'intervento regolatorio

Comunicazione o dichiarazione	Domanda	Documentazione da conservare	Altro
X			

Cosa cambia per il cittadino e/o impresa

Gli operatori economici e professionali sono tenuti, ai sensi degli articoli 35, comma 4, e 55, primo comma, TULPS, a comunicare ogni mese le generalità dei soggetti che hanno acquistato le armi e le munizioni.

L'articolo 11, comma 5, dell'intervento regolatorio sopprime questo obbligo, prevedendo che esso sia assolto direttamente dal SITAM.

III) Denominazione

Obbligo di annotare sui registri ex articoli 35 e 55 TULPS le operazioni compiute riguardanti le armi comuni e le munizioni.

Riferimento normativo interno

Articolo 27 dell'intervento regolatorio

Cosa cambia per il cittadino

Con l'adozione del presente intervento regolatorio, viene meno l'obbligo di annotare sul registro cartaceo le operazioni compiute giornalmente aventi ad oggetto le armi e le munizioni.

IV) Denominazione

Obbligo di versamento dei registri cartacei ex articoli 35 e 55 TULPS alla Questura, al momento della cessazione dell'attività di impresa e professionale riguardante le armi e le munizioni.

Riferimento normativo interno

Articolo 11, comma 3, decreto legislativo 10 agosto 2018, n. 104

Articoli 11, comma 5, e 24, comma 5, dell'intervento regolatorio

Comunicazione o dichiarazione	Domanda	Documentazione da conservare	Altro
			X

Cosa cambia per il cittadino e/o impresa

La sostituzione dei registri su supporto cartaceo con l'immissione dei dati nel SITAM istituito presso il Dipartimento della pubblica sicurezza del Ministero dell'interno determina, conseguentemente, il venir meno dell'adempimento di cui trattasi, a carico degli operatori economici, di versare i predetti registri cartacei alle Questure.

ONERI INTRODOTTI

I) Denominazione

Richiesta di abilitazione per il collegamento al SITAM

Riferimento normativo interno

Articolo 11, commi 1 e 3, decreto legislativo 10 agosto 2018, n. 104

Articolo 13, comma 1, dell'intervento regolatorio

Comunicazione o dichiarazione	Domanda	Documentazione da conservare	Altro
	X		

Cosa cambia per il cittadino e/o impresa

L'obbligo di richiedere l'abilitazione per il collegamento al SITAM costituisce un onere informativo di nuova introduzione.

Esso deriva dal criterio direttivo dettato dall'articolo 11, commi 1 e 3, del decreto legislativo n. 104/2018, secondo cui gli «armaioli» e gli «intermediari» adempiono validamente agli obblighi di registrazione stabiliti dagli articoli 35 e 55 TULPS attraverso l'immissione dei dati nel SITAM.

L'intervento regolatorio prevede che, per effettuare tale immissione, gli «armaioli» e gli «intermediari» debbano richiedere alla Questura territorialmente competente un'abilitazione al collegamento al SITAM.

L'abilitazione è concessa previa la semplice verifica del fatto che il richiedente rientri effettivamente nelle categorie di operatori economici e professionali riconducibili alle nozioni di «armaiolo» e «intermediario», postulate dall'articolo 2, comma 1, lettere *d)* e *p)* dell'intervento regolatorio.

II) Denominazione

Comunicazione mensile delle operazioni effettuate da parte degli utenti titolari di un regime di identificazione elettronica non notificato dallo Stato membro

Riferimento normativo

Articolo 17, comma 4, dell'intervento regolatorio

Comunicazione o dichiarazione	Domanda	Documentazione da conservare	Altro
X			

Cosa cambia per il cittadino e/o impresa

L'articolo 17, comma 4, dell'intervento regolatorio stabilisce che l'«armaiolo» o l'«intermediario» che non ha l'abilitazione per l'accesso al SITAM in quanto titolare di un regime di identificazione elettronica non ancora notificato dallo Stato membro ai sensi dell'articolo 9 del Regolamento UE 910/2014, continua a tenere il registro delle operazioni giornaliere di cui agli articoli 35 e 55 TULPS e adempie alla comunicazione mensile prevista dai medesimi articoli 35 e 55 TULPS su supporto informatico sottoscritto con firma qualificata secondo le modalità indicate nella «home page» del relativo «sito web».

Poiché la comunicazione mensile e la tenuta del registro delle operazioni giornaliere rappresentano obblighi già previsti dai richiamati articoli 35 e 55 TULPS, la disposizione in esame, più che un obbligo informativo di nuova introduzione, costituisce la modalità esecutiva di un onere già sussistente.

Ed invero, l'articolo 17, comma 4, del presente regolamento, da un lato conferma gli obblighi già esistenti in capo ai suindicati operatori economici di tenuta del registro e della comunicazione mensile e, dall'altro, introduce nuove modalità di adempimento della comunicazione su supporto informatico sottoscritto con firma qualificata secondo le modalità indicate nella «home page» del relativo «sito web».

III) Denominazione

Comunicazione dello smarrimento o del furto delle credenziali di accesso al SITAM

Riferimento normativo interno

Articolo 26, comma 5, dell'intervento regolatori

Comunicazione o dichiarazione	Domanda	Documentazione da conservare	Altro
X			

Cosa cambia per il cittadino e/o impresa

L'articolo 26, comma 5, dell'intervento regolatorio introduce in capo ai titolari delle credenziali di accesso al SITAM un nuovo adempimento, consistente nell'obbligo di segnalare immediatamente all'articolazione competente per la gestione del SITAM (allocata nella Questura) l'eventuale furto o smarrimento delle medesime credenziali.

IV) Denominazione

Obbligo per gli utenti di immettere nel SITAM i dati relativi alle operazioni aventi ad oggetto armi e munizioni

Riferimento normativo interno

Articolo 27, comma 1, dell'intervento regolatorio

Articolo 31, comma 1, dell'intervento regolatorio

Comunicazione o dichiarazione	Domanda	Documentazione da conservare	Altro
X			

Cosa cambia per il cittadino e/o impresa

L'articolo 27, comma 1, dell'intervento regolatorio sostituisce con l'immissione nel SITAM delle informazioni di cui agli Allegati A, B e C, l'obbligo di annotare su registri cartacei i dati di cui agli articoli 35 e 55 TULPS riguardanti le operazioni aventi ad oggetto armi e munizioni. L'articolo 31 prevede che, in caso di malfunzionamento del SITAM, tale comunicazione sia assolta temporaneamente con la registrazione dei dati su supporti cartacei o informatici conformi agli standard di sicurezza.

NOTE

AVVERTENZA:

Il testo delle note qui pubblicato è stato redatto dall'amministrazione competente per materia, ai sensi dell'art. 10, comma 3, del testo unico delle disposizioni sulla promulgazione delle leggi, sull'emanazione dei decreti del Presidente della Repubblica e sulle pubblicazioni ufficiali della Repubblica italiana, approvato con D.P.R. 28 dicembre 1985, n. 1092, al solo fine di facilitare la lettura delle disposizioni di legge modificate o alle quali è operato il rinvio. Restano invariati il valore e l'efficacia degli atti legislativi qui trascritti.

Per le direttive CEE vengono forniti gli estremi di pubblicazione nella *Gazzetta Ufficiale* delle Comunità europee (GUUE).

Note alle premesse:

— L'art. 117, secondo comma, lettera *h)* della Costituzione conferisce allo Stato la legislazione esclusiva nella materia dell'ordine pubblico e sicurezza, ad esclusione della polizia amministrativa locale.

— Si riporta il testo dell'art. 17, comma 3, della legge 23 agosto 1988, n. 400 (Disciplina dell'attività di Governo e ordinamento della Presidenza del Consiglio dei Ministri):

«Art. 17 *(Regolamenti)*. — Omissis

3. Con decreto ministeriale possono essere adottati regolamenti nelle materie di competenza del ministro o di autorità sottordinate al ministro, quando la legge espressamente conferisca tale potere. Tali regolamenti, per materie di competenza di più ministri, possono essere adottati con decreti interministeriali, ferma restando la necessità di apposita autorizzazione da parte della legge. I regolamenti ministeriali ed interministeriali non possono dettare norme contrarie a quelle dei regolamenti emanati dal Governo. Essi debbono essere comunicati al Presidente del Consiglio dei ministri prima della loro emanazione.

Omissis.»

— Per il testo dell'art. 11, comma 6, del decreto legislativo 10 agosto 2018, n. 104 (Attuazione della direttiva (UE) 2017/853 del Parlamento europeo e del Consiglio, del 17 maggio 2017, che modifica la direttiva 91/477/CEE del Consiglio, relativa al controllo dell'acquisizione e della detenzione di armi), v. nelle note all'art. 1.

— Si riporta il testo dell'articolo 8 della legge 1° aprile 1981, n. 121 (Nuovo ordinamento dell'Amministrazione della pubblica sicurezza):

«Art. 8 *(Istituzione del Centro elaborazione dati)*. — È istituito presso il Ministero dell'interno, nell'ambito dell'ufficio di cui alla lettera *c)* del primo comma dell'articolo 5, il Centro elaborazione dati, per la raccolta delle informazioni e dei dati di cui all'articolo 6, lettera *a)*, e all'articolo 7.

Il Centro provvede alla raccolta, elaborazione, classificazione e conservazione negli archivi magnetici delle informazioni e dei dati nonché alla loro comunicazione ai soggetti autorizzati, indicati nell'articolo 9, secondo i criteri e le norme tecniche fissati ai sensi del comma seguente.

Con decreto del Ministro dell'interno è costituita una commissione tecnica, presieduta dal funzionario preposto all'ufficio di cui alla lettera *c)* del primo comma dell'articolo 5, per la fissazione dei criteri e delle norme tecniche per l'espletamento da parte del Centro delle operazioni di cui al comma precedente e per il controllo tecnico sull'osservanza di tali criteri enorme da parte del personale operante presso il Centro stesso. I criteri e le norme tecniche predetti divengono esecutivi con l'approvazione del Ministro dell'interno.»

— Il regolamento (CE) del 23 luglio 2014, n. 910 (pubblicato nella *G.U.* della Unione Europea n. L 257 del 28 agosto 2014), reca: «Regolamento del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE».

— La direttiva del 18 giugno 1991, n. 91/477/CEE (pubblicata nella G.U.C.E. del 13 settembre 1991, n. L 256) reca: «Direttiva del Consiglio relativa al controllo dell'acquisizione e della detenzione di armi».

— La direttiva del 24 marzo 2021, n. 2021/555 (pubblicata nella G.U.U.E. del 6 aprile 2021, n. L 115) reca: «Regolamento del Parlamento europeo e del Consiglio relativa al controllo dell'acquisizione e della detenzione di armi» (codificazione)».

— Il regolamento (CE) del 16 gennaio 2019, n. 2019/686/UE (pubblicato nella G.U.U.E. del 3 maggio 2019), n. L 116 reca: «Regolamento delegato della commissione che stabilisce le modalità dettagliate, a norma della direttiva 91/477/CEE del Consiglio, per lo scambio sistematico, con mezzi elettronici di informazioni relative al trasferimento di armi da fuoco nell' Unione».

— Si riporta il testo degli articoli 5 e 25 della legge 18 aprile 1975, n. 110 (Norme integrative della disciplina vigente per il controllo delle armi, delle munizioni e degli esplosivi):

«Art. 5 (*Limiti alle registrazioni. Divieto di strumenti trasformabili in armi)*. — 1. Le disposizioni di cui al primo comma dell'articolo 55 del testo unico delle leggi di pubblica sicurezza 18 giugno 1931, n. 773 e successive modificazioni, non si applicano alla vendita al minuto delle cartucce da caccia a pallini, dei relativi bossoli o inneschi nonché alla vendita dei pallini per le armi ad aria compressa.

2. L'articolo 4-*bis* del decreto-legge 22 novembre 1956, n. 1274, convertito nella legge 22 dicembre 1956, n. 1452, è abrogato.

3. Le disposizioni del citato testo unico, del regio decreto 6 maggio 1940, n. 635, e quelle della presente legge non si applicano agli strumenti di cui al presente articolo.

4. Gli strumenti riproducenti armi non possono essere fabbricati con l'impiego di tecniche e di materiali che ne consentano la trasformazione in armi da guerra o comuni da sparo o che consentano l'utilizzo del relativo munizionamento o il lancio di oggetti idonei all'offesa della persona. I predetti strumenti se realizzati in metallo devono avere la canna completamente ostruita, non in grado di camerare cartucce ed avere la canna occlusa da un tappo rosso inamovibile. Quelli da segnalazione acustica, destinati a produrre un rumore tramite l'accensione di una cartuccia a salve, devono avere la canna occlusa da un inserto di metallo ed un tappo rosso inamovibile all'estremità della canna.

Gli strumenti denominati «softair», vendibili solo ai maggiori di 16 anni, possono sparare pallini in plastica, di colore vivo, per mezzo di aria o gas compresso, purché l'energia del singolo pallino, misurata ad un metro dalla volata, non sia superiore ad 1 joule. La canna dell'arma deve essere colorata di rosso per almeno tre centimetri e qualora la canna non sia sporgente la verniciatura deve interessare la parte anteriore dello strumento per un pari tratto.

Gli strumenti di cui al presente comma sono sottoposti, a spese dell'interessato, a verifica di conformità accertata dal Banco nazionale di prova.

5. Nessuna limitazione è posta all'aspetto degli strumenti riproducenti armi destinati all'esportazione.

6. Chiunque produce o pone in commercio gli strumenti di cui al presente articolo, senza l'osservanza delle disposizioni del quarto comma, è punito con la reclusione da uno a tre anni e con la multa da 1.500 euro a 15.000 euro.

7. Quando l'uso o il porto d'armi è previsto quale elemento costitutivo o circostanza aggravante del reato, il reato stesso sussiste o è aggravato anche qualora si tratti di arma per uso scenico o di strumenti riproducenti armi la cui canna non sia occlusa a norma del quarto comma.»

«Art. 25 *(Registro delle operazioni giornaliere)*. — 1. Chiunque, per l'esercizio della propria attività lavorativa, fa abituale impiego di esplosivi di qualsiasi genere deve tenere il registro delle operazioni giornaliere previsto dal primo comma dell'articolo 55 del testo unico delle leggi di pubblica sicurezza 18 giugno 1931, n. 773.

2. E' punito con la reclusione da sei mesi a tre anni e con la multa da euro 206 (lire 400.000) a euro 2.065 (lire 4.000.000) chi non osserva l'obbligo di cui al comma precedente.

3. Con la stessa pena sono punite le persone indicate nel primo comma del citato articolo 55 che non osservano l'obbligo di tenuta del registro.

4. Sono punite con l'arresto da venti giorni a tre mesi e con l'ammenda fino a euro 103 (lire 200.000) le persone obbligate a tenere il predetto registro le quali rifiutano ingiustificatamente di esibire il registro stesso agli ufficiali ed agenti di pubblica sicurezza che ne facciano richiesta.».

— Si riporta il testo dell'articolo 55 del regio decreto 18 giugno 1931, n. 773 (Approvazione del testo unico delle leggi di pubblica sicurezza):

«Art. 55. Gli esercenti fabbriche, depositi o rivendite di esplodenti di qualsiasi specie sono obbligati a tenere un registro delle operazioni giornaliere, in cui saranno indicate le generalità delle persone con le quali le operazioni stesse sono compiute. Il registro è tenuto in formato elettronico, secondo le modalità definite nel regolamento. I rivenditori di materie esplodenti devono altresì comunicare mensilmente all'ufficio di polizia competente per territorio le generalità delle persone e delle ditte che hanno acquistato munizioni ed esplosivi, la specie, i contrassegni e la quantità delle munizioni e degli esplosivi venduti e gli estremi dei titoli abilitativi all'acquisto esibiti dagli interessati.

Tale registro deve essere esibito a ogni richiesta degli ufficiali od agenti di pubblica sicurezza e deve essere conservato per un periodo di cinquanta anni anche dopo la cessazione dell'attività.

Alla cessazione dell'attività, i registri delle operazioni giornaliere, sia in formato cartaceo che elettronico, devono essere consegnati all'Autorità di pubblica sicurezza che aveva rilasciato la licenza, che ne curerà la conservazione per il periodo necessario. Le informazioni registrate nel sistema informatico di cui all'articolo 3 del decreto legislativo 25 gennaio 2010, n. 8, devono essere conservate per i 10 anni successivi alla cessazione dell'attività.

È vietato vendere o in qualsiasi altro modo cedere materie esplodenti di I^{a}, II^{a}, III^{a}, IV^{a} e V^{a} categoria, gruppo A e gruppo B, a priva-

ti che non siano muniti di permesso di porto d'armi ovvero di nulla osta rilasciato dal Questore, nonché materie esplodenti di Vª categoria, gruppo C, a privati che non siano maggiorenni e che non esibiscano un documento di identità in corso di validità. Il nulla osta non può essere rilasciato a minori: ha la validità di un mese ed è esente da ogni tributo. La domanda è redatta in carta libera.

Il Questore può subordinare il rilascio del nulla osta di cui al comma precedente, alla presentazione di certificato del medico provinciale, o dell'ufficiale sanitario o di un medico militare, dal quale risulti che il richiedente non è affetto da malattie mentali oppure da vizi che ne diminuiscono, anche temporaneamente, la capacità di intendere e di volere. Il contravventore è punito con l'arresto da nove mesi a tre anni e con l'ammenda non inferiore a euro 154 (lire 300.000).

Gli obblighi di registrazione delle operazioni giornaliere e di comunicazione mensile all'ufficio di polizia competente per territorio non si applicano alle materie esplodenti di Vª categoria, gruppo D e gruppo E. L'acquirente o cessionario di materie esplodenti in violazione delle norme del presente articolo è punito con l'arresto sino a diciotto mesi e con l'ammenda sino a euro 154 (lire 300.000).»

— Si riporta il testo degli articoli 9 e 10 della legge 1° aprile 1981, n. 121 (Nuovo ordinamento dell'Amministrazione della pubblica sicurezza):

«Art. 9 *(Accesso ai dati ed informazioni e loro* uso). — L'accesso ai dati e alle informazioni conservati negli archivi automatizzati del Centro di cui all'articolo precedente e la loro utilizzazione sono consentiti agli ufficiali di polizia giudiziaria appartenenti alle forze di polizia, agli ufficiali di pubblica sicurezza e ai funzionari dei servizi di sicurezza, nonché agli agenti di polizia giudiziaria delle forze di polizia debitamente autorizzati ai sensi del secondo comma del successivo articolo 11.

L'accesso ai dati e alle informazioni di cui al comma precedente è consentito all'autorità giudiziaria ai fini degli accertamenti necessari per i procedimenti in corso e nei limiti stabiliti dal codice di procedura penale.

È comunque vietata ogni utilizzazione delle informazioni e dei dati predetti per finalità diverse da quelle previste dall'articolo 6, lettera *a)*. È altresì vietata ogni circolazione delle informazioni all'interno della pubblica amministrazione fuori dei casi indicati nel primo comma del presente articolo.»

«Art. 10 (*Controlli)*. — 1. Il controllo sul Centro elaborazione dati è esercitato dal Garante per la protezione dei dati personali, nei modi previsti dalla legge e dai regolamenti.

2. I dati e le informazioni conservati negli archivi del Centro possono essere utilizzati in procedimenti giudiziari o amministrativi soltanto attraverso l'acquisizione delle fonti originarie indicate nel primo comma dell'articolo 7, fermo restando quanto stabilito dall'articolo 240 del codice di procedura penale. Quando nel corso di un procedimento giurisdizionale o amministrativo viene rilevata l'erroneità o l'incompletezza dei dati e delle informazioni, o l'illegittimità del loro trattamento, l'autorità precedente ne dà notizia al Garante per la protezione dei dati personali.

3. La persona alla quale si riferiscono i dati può chiedere all'ufficio di cui alla lettera *c)* del primo comma dell'articolo 5 la conferma dell'esistenza di dati personali che lo riguardano, la loro comunicazione in forma intellegibile e, se i dati risultano trattati in violazione di vigenti disposizioni di legge o di regolamento, la loro cancellazione o trasformazione in forma anonima.

4. Esperiti i necessari accertamenti, l'ufficio comunica al richiedente, non oltre trenta giorni dalla richiesta, le determinazioni adottate. L'ufficio può omettere di provvedere sulla richiesta se ciò può pregiudicare azioni od operazioni a tutela dell'ordine e della sicurezza pubblica o di prevenzione e repressione della criminalità, dandone informazione al Garante per la protezione dei dati personali.

5. Chiunque viene a conoscenza dell'esistenza di dati personali che lo riguardano, trattati anche in forma non automatizzata in violazione di disposizioni di legge o di regolamento, può chiedere al tribunale del luogo ove risiede il titolare del trattamento di compiere gli accertamenti necessari e di ordinare la rettifica, l'integrazione, la cancellazione o la trasformazione in forma anonima dei dati medesimi.».

— Si riporta il testo dell'art. 21, comma 1, della legge 26 marzo 2001, n. 128 (Interventi legislativi in materia di tutela della sicurezza dei cittadini):

«Art. 21. — 1. Ai fini di cui all'articolo 6 della legge 1º aprile 1981, n. 121, le Forze di polizia conferiscono senza ritardo al Centro elaborazione dati del Dipartimento della pubblica sicurezza, istituito dall'articolo 8 della medesima legge, le notizie e le informazioni acquisite nel corso delle attività di prevenzione e repressione dei reati e di quelle amministrative.

Omissis.»

— Il decreto legislativo 30 dicembre 1992, n. 527, recante: "Attuazione della direttiva 91/477/CEE relativa al controllo dell'acquisizione e della detenzione di armi" è pubblicato nella *Gazzetta Ufficiale* 11 gennaio 1993, n. 7, S.O..

— 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» è pubblicato nella *Gazzetta Ufficiale* 24 maggio 2018, n. 119.

.

— Si riporta il testo dell'articolo 35 del regio decreto 18 giugno 1931, n. 773 (Approvazione del testo unico delle leggi di pubblica sicurezza):

«Art. 35. — 1. L'armaiolo di cui all'articolo 1-*bis*, comma 1, lettera *g)*, del decreto legislativo 30 dicembre 1992, n. 527, è obbligato a tenere un registro delle operazioni giornaliere, nel quale devono essere indicate le generalità delle persone con cui le operazioni stesse sono compiute. Il registro è tenuto in formato elettronico, secondo le modalità definite nel regolamento.

2. Il registro di cui al comma 1 deve essere esibito a richiesta degli ufficiali od agenti di pubblica sicurezza e deve essere conservato per un periodo di 50 anni.

3. Alla cessazione dell'attività, i registri delle operazioni giornaliere, sia in formato cartaceo che elettronico, devono essere consegnati all'Autorità di pubblica sicurezza che aveva rilasciato la licenza, che ne cura la conservazione per il periodo necessario. Le informazioni registrate nel sistema informatico di cui all'articolo 3 del decreto legislativo del 25 gennaio 2010, n. 8, sono conservate per i 50 anni successivi alla cessazione dell'attività.

4. Gli armaioli devono, altresì, comunicare mensilmente all'ufficio di polizia competente per territorio le generalità dei privati che hanno acquistato o venduto loro le armi, nonché la specie e la quantità delle armi vendute o acquistate e gli estremi dei titoli abilitativi all'acquisto esibiti dagli interessati. Le comunicazioni possono essere trasmesse anche per via telematica.

5. E' vietato vendere o in qualsiasi altro modo cedere armi a privati che non siano muniti di permesso di porto d'armi ovvero di nulla osta all'acquisto rilasciato dal Questore.

6. Il nulla osta non può essere rilasciato ai minori di 18 anni, ha la validità di un mese ed è esente da ogni tributo. La domanda è redatta in carta libera.

7. Il Questore subordina il rilascio del nulla osta alla presentazione di certificato rilasciato dal settore medico legale delle Aziende sanitarie locali, o da un medico militare, della Polizia di Stato o del Corpo nazionale dei vigili del fuoco, dal quale risulti che il richiedente non è affetto da malattie mentali oppure da vizi che ne diminuiscono, anche temporaneamente, la capacità di intendere e di volere, ovvero non risulti assumere, anche occasionalmente, sostanze stupefacenti o psicotrope ovvero abusare di alcool, nonché dalla presentazione di ogni altra certificazione sanitaria prevista dalle disposizioni vigenti.

8. Il contravventore è punito con l'arresto da sei mesi a due anni e con l'ammenda da 4.000 euro a 20.000 euro.

9. L'acquirente o cessionario di armi in violazione delle norme del presente articolo è punito con l'arresto fino a un anno e con l'ammenda da 2.000 euro a 10.000 euro.

10. Il provvedimento con cui viene rilasciato il nulla osta all'acquisto delle armi, nonché quello che consente l'acquisizione, a qualsiasi titolo, della disponibilità di un'arma devono essere comunicati, a cura dell'interessato, ai conviventi maggiorenni, anche diversi dai familiari, compreso il convivente more uxorio, individuati dal regolamento e indicati dallo stesso interessato all'atto dell'istanza, secondo le modalità definite nel medesimo regolamento. In caso di violazione degli obblighi previsti in attuazione del presente comma, si applica la sanzione amministrativa da 2.000 euro a 10.000 euro. Può essere disposta, altresì, la revoca della licenza o del nulla osta alla detenzione.»

— Si riporta il testo dell'articolo 1-*bis*, comma 1, lettera *f)* e *g)* del decreto legislativo 30 dicembre 1992, n. 527 (Attuazione della direttiva 91/477/CEE relativa al controllo dell'acquisizione e della detenzione di armi):

«Art. 1-*bis*. — 1. Ai fini del presente decreto, si intende per:

omissis

f) «intermediario«, qualsiasi persona fisica o giuridica, diversa dall'armaiolo e dai soggetti che esercitano la sola attività di trasporto, che svolge, pur senza avere la materiale disponibilità di armi da fuoco, loro parti o munizioni, un'attività professionale consistente integralmente o in parte:

1) nella negoziazione o organizzazione di transazioni dirette all'acquisto, alla vendita o alla fornitura di armi da fuoco, loro parti o munizioni;

2) nell'organizzazione del trasferimento di armi da fuoco, loro parti o munizioni all'interno del territorio nazionale o di altro Stato membro, dallo Stato italiano ad altro Stato anche terzo e viceversa o fra uno Stato membro e un altro Stato anche terzo e viceversa;

g) «armaiolo», qualsiasi persona fisica o giuridica che esercita un'attività professionale consistente integralmente o in parte in una o più attività fra le seguenti:

1) fabbricazione, commercio, scambio, assemblaggio, locazione, riparazione, disattivazione, modifica o trasformazione di armi da fuoco o loro parti;

2) fabbricazione, commercio, scambio, modifica o trasformazione di munizioni.»

— Il regio decreto 6 maggio 1940, n. 635, reca: «Approvazione del regolamento per l'esecuzione del testo unico 18 giugno 1931, n. 773, delle leggi di pubblica sicurezza» è pubblicato nella Gazz. Uff. 26 giugno 1940, n. 149, S.O.

— Si riporta il testo dell'articolo 1 del 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»:

«Art. 1 *(Perimetro di sicurezza nazionale cibernetica)*. — 1. Al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori pubblici e privati aventi una sede nel territorio nazionale, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale, è istituito il perimetro di sicurezza nazionale cibernetica.

2. Entro quattro mesi dalla data di entrata in vigore della legge di conversione del presente decreto, con decreto del Presidente del Consiglio dei ministri, adottato su proposta del Comitato interministeriale per la cybersicurezza (CIC):

a) sono definiti modalità e criteri procedurali di individuazione di amministrazioni pubbliche, enti e operatori pubblici e privati di cui al comma 1 aventi una sede nel territorio nazionale, inclusi nel perimetro di sicurezza nazionale cibernetica e tenuti al rispetto delle misure e degli obblighi previsti dal presente articolo; ai fini dell'individuazione, fermo restando che per gli Organismi di informazione per la sicurezza si applicano le norme previste dalla legge 3 agosto 2007, n. 124, si procede sulla base dei seguenti criteri:

1) il soggetto esercita una funzione essenziale dello Stato, ovvero assicura un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato;

2) l'esercizio di tale funzione o la prestazione di tale servizio dipende da reti, sistemi informativi e servizi informatici;

2-*bis*) l'individuazione avviene sulla base di un criterio di gradualità, tenendo conto dell'entità del pregiudizio per la sicurezza nazionale che, in relazione alle specificità dei diversi settori di attività, può derivare dal malfunzionamento, dall'interruzione, anche parziali, ovvero dall'utilizzo improprio delle reti, dei sistemi informativi e dei servizi informatici predetti;

b) sono definiti, sulla base di un'analisi del rischio e di un criterio di gradualità che tenga conto delle specificità dei diversi settori di attività, i criteri con i quali i soggetti di cui al comma 2-*bis* predispongono e aggiornano con cadenza almeno annuale un elenco delle reti, dei sistemi informativi e dei servizi informatici di cui al comma 1, di rispettiva pertinenza, comprensivo della relativa architettura e componentistica, fermo restando che, per le reti, i sistemi informativi e i servizi informatici attinenti alla gestione delle informazioni classificate, si applica quanto previsto dal regolamento adottato ai sensi dell'articolo 4, comma 3, lettera *l)*, della legge 3 agosto 2007, n. 124; all'elaborazione di tali criteri provvede, adottando opportuni moduli organizzativi, il Tavolo interministeriale di cui all'articolo 6 del regolamento di cui al decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131; entro sei mesi dalla data della comunicazione, prevista dal comma 2-*bis*, a ciascuno dei soggetti iscritti nell'elenco di cui al medesimo comma, i soggetti pubblici e quelli di cui all'articolo 29 del codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, nonché quelli privati, di cui al citato comma 2-*bis*, trasmettono tali elenchi all'Agenzia per la cybersicurezza nazionale, anche per le attività di prevenzione, preparazione e gestione di crisi cibernetiche affidate al Nucleo per la cybersicurezza; il Dipartimento delle informazioni per la sicurezza, l'Agenzia informazioni e sicurezza esterna (AISE) e l'Agenzia informazioni e sicurezza interna (AISI) ai fini dell'esercizio delle funzioni istituzionali previste dagli articoli 1, comma 3-*bis*, 4, 6 e 7 della legge n. 124 del 2007, nonché l'organo del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione di cui all'articolo 7-*bis* del decreto- legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155, accedono a tali elenchi per il tramite della piattaforma digitale di cui all'articolo 9, comma 1, del regolamento di cui al decreto del Presidente del Consiglio dei ministri n. 131 del 2020, costituita presso l'Agenzia per la cybersicurezza nazionale

2-*bis*. L'elencazione dei soggetti individuati ai sensi del comma 2, lettera *a)*, è contenuta in un atto amministrativo, adottato dal Presidente del Consiglio dei ministri, su proposta del CIC, entro trenta giorni dalla data di entrata in vigore del decreto del Presidente del Consiglio dei ministri di cui al comma 2. Il predetto atto amministrativo, per il quale è escluso il diritto di accesso, non è soggetto a pubblicazione, fermo restando che a ciascun soggetto è data, separatamente, comunicazione senza ritardo dell'avvenuta iscrizione nell'elenco. L'aggiornamento del predetto atto amministrativo è effettuato con le medesime modalità di cui al presente comma.

2-*ter*. Gli elenchi dei soggetti di cui alla lettera *a)* del comma 2 del presente articolo sono trasmessi al Dipartimento delle informazioni per la sicurezza, che provvede anche a favore dell'AISE e dell'AISI ai fini dell'esercizio delle funzioni istituzionali previste dagli articoli 1, comma 3-*bis*, 4, 6 e 7 della legge 3 agosto 2007, n. 124.

3. Entro dieci mesi dalla data di entrata in vigore della legge di conversione del presente decreto, con decreto del Presidente del Consiglio dei ministri, che disciplina altresì i relativi termini e modalità attuative, adottato su proposta del CIC:

a) sono definite le procedure secondo cui i soggetti di cui al comma 2-*bis* notificano gli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui al comma 2, lettera *b)*, al Gruppo di intervento per la sicurezza informatica in caso di incidente (CSIRT) Italia, che inoltra tali notifiche, tempestivamente, al Dipartimento delle informazioni per la sicurezza anche per le attività demandate al Nucleo per la sicurezza cibernetica; il Dipartimento delle informazioni per la sicurezza assicura la trasmissione delle notifiche così ricevute all'organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione di cui all'articolo 7-*bis* del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155, nonché alla Presidenza del Consiglio dei ministri, se provenienti da un soggetto pubblico o da un soggetto di cui all'articolo 29 del decreto legislativo 7 marzo 2005, n. 82, ovvero al Ministero dello sviluppo economico, se effettuate da un soggetto privato;

b) sono stabilite misure volte a garantire elevati livelli di sicurezza delle reti, dei sistemi informativi e dei servizi informatici di cui al comma 2, lettera *b)*, tenendo conto degli standard definiti a livello internazionale e dell'Unione europea relative:

1) alla struttura organizzativa preposta alla gestione della sicurezza;

1-*bis*) alle politiche di sicurezza e alla gestione del rischio;

2) alla mitigazione e gestione degli incidenti e alla loro prevenzione, anche attraverso interventi su apparati o prodotti che risultino gravemente inadeguati sul piano della sicurezza;

3) alla protezione fisica e logica e dei dati;

4) all'integrità delle reti e dei sistemi informativi;

5) alla gestione operativa, ivi compresa la continuità del servizio;

6) al monitoraggio, test e controllo;

7) alla formazione e consapevolezza;

8) all'affidamento di forniture di beni, sistemi e servizi di information and communication technology (ICT), anche mediante definizione di caratteristiche e requisiti di carattere generale, di standard e di eventuali limiti.

3-*bis*. Al di fuori dei casi di cui al comma 3, i soggetti di cui al comma 2-*bis* notificano gli incidenti di cui all'articolo 1, comma 1, lettera *h)*, del regolamento di cui al decreto del Presidente del Consiglio dei ministri 14 aprile 2021, n. 81, aventi impatto su reti, sistemi informativi e servizi informatici di propria pertinenza diversi da quelli di cui al comma 2, lettera *b)*, del presente articolo, fatta eccezione per quelli aventi impatto sulle reti, sui sistemi informativi e sui servizi informatici del Ministero della difesa, per i quali si applicano i princìpi e le modalità di cui all'articolo 528, comma 1, lettera *d)*, del codice di cui al decreto legislativo 15 marzo 2010, n. 66. I medesimi soggetti effettuano la notifica entro il termine di settantadue ore. Si applicano, per la decorrenza del termine e per le modalità di notifica, in quanto compatibili, le disposizioni dell'articolo 3, comma 4, secondo e terzo periodo, del regolamento di cui al decreto del Presidente del Consiglio dei ministri 14 aprile 2021, n. 81. Si applicano, altresì, le disposizioni di cui all'articolo 4, commi 2 e 4, del medesimo regolamento. Con determinazioni tecniche del direttore generale, sentito il vice direttore generale, dell'Agenzia per la cybersicurezza nazionale, è indicata la tassonomia degli incidenti che debbono essere oggetto di notifica ai sensi del presente comma e possono essere dettate specifiche modalità di notifica.

4. All'elaborazione delle misure di cui al comma 3, lettera *b)*, provvedono, secondo gli ambiti di competenza delineati dal presente decreto, il Ministero dello sviluppo economico e la Presidenza del Consiglio dei ministri, d'intesa con il Ministero della difesa, il Ministero dell'interno, il Ministero dell'economia e delle finanze e il Dipartimento delle informazioni per la sicurezza.

4-*bis*. Gli schemi dei decreti di cui ai commi 2 e 3 sono trasmessi alla Camera dei deputati e al Senato della Repubblica per l'espressione del parere delle Commissioni parlamentari competenti per materia, che si pronunciano nel termine di trenta giorni, decorso il quale il decreto può essere comunque adottato. I medesimi schemi sono altresì trasmessi al Comitato parlamentare per la sicurezza della Repubblica.

4-*ter*. L'atto amministrativo di cui al comma 2-*bis* e i suoi aggiornamenti sono trasmessi, entro dieci giorni dall'adozione, al Comitato parlamentare per la sicurezza della Repubblica.

5. Per l'aggiornamento di quanto previsto dai decreti di cui ai commi 2 e 3 si procede secondo le medesime modalità di cui ai commi 2, 3, 4 e 4-*bis* con cadenza almeno biennale.

6. Con regolamento, adottato ai sensi dell'articolo 17, comma 1, della legge 23 agosto 1988, n. 400, entro dieci mesi dalla data di entrata in vigore della legge di conversione del presente decreto, sono disciplinati le procedure, le modalità e i termini con cui:

a) i soggetti di cui al comma 2-*bis*, che intendano procedere, anche per il tramite delle centrali di committenza alle quali essi sono tenuti a fare ricorso ai sensi dell'articolo 1, comma 512, della legge 28 dicembre 2015, n. 208, all'affidamento di forniture di beni, sistemi e servizi ICT destinati a essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici di cui al comma 2, lettera *b)*, appartenenti a categorie individuate, sulla base di criteri di natura tecnica, con decreto del Presidente del Consiglio dei ministri, da adottare entro dieci mesi dalla data di entrata in vigore della legge di conversione del presente decreto, ne danno comunicazione al Centro di valutazione e certificazione nazionale (CVCN), istituito presso il Ministero dello sviluppo economico; la comunicazione comprende anche la valutazione del rischio associato all'oggetto della fornitura, anche in relazione all'ambito di impiego. L'obbligo di comunicazione di cui alla presente lettera è efficace a decorrere dal trentesimo giorno successivo alla pubblicazione nella *Gazzetta Ufficiale* della Repubblica italiana del decreto del Presidente del Consiglio dei ministri che, sentita l'Agenzia per la cybersicurezza nazionale, attesta l'operatività del CVCN e comunque dal 30 giugno 2022. Entro quarantacinque giorni dalla ricezione della comunicazione, prorogabili di quindici giorni, una sola volta, in caso di particolare complessità, il CVCN può effettuare verifiche preliminari ed imporre condizioni e test di hardware e software da compiere anche in collaborazione con i soggetti di cui al comma 2-*bis*, secondo un approccio gradualmente crescente nelle verifiche di sicurezza. Decorso il termine di cui al precedente periodo senza che il CVCN si sia pronunciato, i soggetti che hanno effettuato la comunicazione possono proseguire nella procedura di affidamento. In caso di imposizione di condizioni e test di hardware e software, i relativi bandi di gara e contratti sono integrati con clausole che condizionano, sospensivamente ovvero risolutivamente, il contratto al rispetto delle condizioni e all'esito favorevole dei test disposti dal CVCN. I test devono essere conclusi nel termine di sessanta giorni. Decorso il termine di cui al precedente periodo, i soggetti che hanno effettuato la comunicazione possono proseguire nella procedura di affidamento. In relazione alla specificità delle forniture di beni, sistemi e servizi ICT da impiegare su reti, sistemi informativi e servizi informatici del Ministero dell'interno e del Ministero della difesa, individuati ai sensi del comma 2, lettera *b)*, i predetti Ministeri, nell'ambito delle risorse umane e finanziarie disponibili a legislazione vigente e senza nuovi o maggiori oneri a carico della finanza pubblica, in coerenza con quanto previsto dal presente decreto, possono procedere, con le medesime modalità e i medesimi termini previsti dai periodi precedenti, attraverso la comunicazione ai propri Centri di valutazione accreditati per le attività di cui al presente decreto, ai sensi del comma 7, lettera *b)*, che impiegano le metodologie di verifica e di test definite dal CVCN. Per tali casi i predetti Centri informano il CVCN con le modalità stabilite con il decreto del Presidente del Consiglio dei ministri, di cui al comma 7, lettera *b)*. Non sono oggetto di comunicazione gli affidamenti delle forniture di beni, sistemi e servizi ICT destinate alle reti, ai sistemi informativi e ai servizi informatici per lo svolgimento delle attività di prevenzione, accertamento e repressione dei reati e i casi di deroga stabiliti dal medesimo regolamento con riguardo alle forniture di beni, sistemi e servizi ICT per le quali sia indispensabile procedere in sede estera, fermo restando, in entrambi i casi, l'utilizzo di beni, sistemi e servizi ICT conformi ai livelli di sicurezza di cui al comma 3, lettera *b)*, salvo motivate esigenze connesse agli specifici impieghi cui essi sono destinati;

b) i soggetti individuati quali fornitori di beni, sistemi e servizi destinati alle reti, ai sistemi informativi e ai servizi informatici di cui al comma 2, lettera *b)*, assicurano al CVCN e, limitatamente agli ambiti di specifica competenza, ai Centri di valutazione operanti presso i Ministeri dell'interno e della difesa, di cui alla lettera *a)* del presente comma, la propria collaborazione per l'effettuazione delle attività di test di cui alla lettera *a)* del presente comma, sostenendone gli oneri; il CVCN segnala la mancata collaborazione al Ministero dello sviluppo economico, in caso di fornitura destinata a soggetti privati, o alla Presidenza del Consiglio dei ministri, in caso di fornitura destinata a soggetti pubblici ovvero a quelli di cui all'articolo 29 del codice di cui al decreto legislativo 7 marzo 2005, n. 82; sono inoltrate altresì alla Presidenza del Consiglio dei ministri le analoghe segnalazioni dei Centri di valutazione dei Ministeri dell'interno e della difesa, di cui alla lettera *a)*;

c) la Presidenza del Consiglio dei ministri, per i profili di pertinenza dei soggetti pubblici e di quelli di cui all'articolo 29 del codice dell'Amministrazione digitale di cui al decreto legislativo 7 marzo 2005, n. 82, di cui al comma 2-*bis*, e il Ministero dello sviluppo economico, per i soggetti privati di cui al medesimo comma, svolgono attività di ispezione e verifica in relazione a quanto previsto dal comma 2, lettera *b)*, dal comma 3, dal presente comma e dal comma 7, lettera *b)*, impartendo, se necessario, specifiche prescrizioni; nello svolgimento delle predette attività di ispezione e verifica l'accesso, se necessario, a dati o metadati personali e amministrativi è effettuato in conformità a quanto previsto dal regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, e dal codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196; per le reti, i sistemi informativi e i servizi informatici di cui al comma 2, lettera *b)*, connessi alla funzione di prevenzione e repressione dei reati, alla tutela dell'ordine e della sicurezza pubblica, alla difesa civile e alla difesa e sicurezza militare dello Stato, le attività di ispezione e verifica sono svolte, nell'ambito delle risorse umane e finanziarie disponibili a legislazione vigente e senza nuovi o maggiori oneri a carico della finanza pubblica, dalle strutture specializzate in tema di protezione di reti e sistemi, nonché, nei casi in cui siano espressamente previste dalla legge, in tema di prevenzione e di contrasto del crimine informatico, delle amministrazioni da cui dipendono le Forze di polizia e le Forze armate, che ne comunicano gli esiti alla Presidenza del Consiglio dei ministri per i profili di competenza.

7. Nell'ambito dell'approvvigionamento di prodotti, processi, servizi ICT e associate infrastrutture destinati alle reti, ai sistemi informativi e per l'espletamento dei servizi informatici di cui al comma 2, lettera *b)*, il CVCN assume i seguenti compiti:

a) contribuisce all'elaborazione delle misure di sicurezza di cui al comma 3, lettera *b)*, per ciò che concerne l'affidamento di forniture di beni, sistemi e servizi ICT;

b) ai fini della verifica delle condizioni di sicurezza e dell'assenza di vulnerabilità note, anche in relazione all'ambito di impiego, definisce le metodologie di verifica e di test e svolge le attività di cui al comma 6, lettera *a)*, dettando, se del caso, anche prescrizioni di utilizzo al committente; a tali fini il CVCN si avvale anche di laboratori dallo stesso accreditati secondo criteri stabiliti da un decreto del Presidente del Consiglio dei ministri, adottato entro dieci mesi dalla data di entrata in vigore della legge di conversione del presente decreto, su proposta del CIC, impiegando, per le esigenze delle amministrazioni centrali dello Stato, quelli eventualmente istituiti, senza nuovi o maggiori oneri a carico della finanza pubblica, presso le medesime amministrazioni. Con lo stesso decreto sono altresì stabiliti i raccordi, ivi compresi i contenuti, le modalità e i termini delle comunicazioni, tra il CVCN e i predetti laboratori, nonché tra il medesimo CVCN e i Centri di valutazione del Ministero dell'interno e del Ministero della difesa, di cui al comma 6, lettera *a)*, anche la fine di assicurare il coordinamento delle rispettive attività e perseguire la convergenza e la non duplicazione delle valutazioni in presenza di medesimi condizioni e livelli di rischio;

c) elabora e adotta, previo conforme avviso del Tavolo interministeriale di cui all'articolo 6 del decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131, schemi di certificazione cibernetica, tenendo conto degli standard definiti a livello internazionale e dell'Unione europea, laddove, per ragioni di sicurezza nazionale, gli schemi di certificazione esistenti non siano ritenuti adeguati alle esigenze di tutela del perimetro di sicurezza nazionale cibernetica.

8. I soggetti di cui agli articoli 12 e 14 del decreto legislativo 18 maggio 2018, n. 65, e quelli di cui all'articolo 16-*ter*, comma 2, del codice delle comunicazioni elettroniche di cui al decreto legislativo 1° agosto 2003, n. 259, inclusi nel perimetro di sicurezza nazionale cibernetica:

a) osservano le misure di sicurezza previste, rispettivamente, dai predetti decreti legislativi, ove di livello almeno equivalente a quelle adottate ai sensi del comma 3, lettera *b)*, del presente articolo; le eventuali misure aggiuntive necessarie al fine di assicurare i livelli di sicurezza previsti dal presente decreto sono definite dall'Agenzia per la cybersicurezza nazionale, di cui al comma 2-*bis*, e dal Ministero dello sviluppo economico per i soggetti privati di cui al medesimo comma, avvalendosi anche del CVCN; il Ministero dello sviluppo economico e la Presidenza del Consiglio dei ministri si raccordano, ove necessario, con le autorità competenti di cui all'articolo 7 del decreto legislativo 18 maggio 2018, n. 65;

b) assolvono l'obbligo di notifica di cui al comma 3, lettera *a)*, che costituisce anche adempimento, rispettivamente, dell'obbligo di notifica di cui agli articoli 12 e 14 del decreto legislativo 18 maggio 2018, n. 65, e dell'analogo obbligo previsto ai sensi dell'articolo 16-*ter* del codice di cui al decreto legislativo 1° agosto 2003, n. 259, e delle correlate disposizioni attuative; a tal fine, oltre a quanto previsto dal comma 3, lettera *a)*, anche in relazione alle disposizioni di cui all'articolo 16-*ter* del codice di cui al decreto legislativo 1° agosto 2003, n. 259, il CSIRT Italia inoltra le notifiche ricevute ai sensi del predetto comma 3, lettera *a)*, autorità nazionale competente NIS di cui all'articolo 7 del decreto legislativo 18 maggio 2018, n. 65.

9. Salvo che il fatto costituisca reato:

a) il mancato adempimento degli obblighi di predisposizione, di aggiornamento e di trasmissione dell'elenco delle reti, dei sistemi informativi e dei servizi informatici di cui al comma 2, lettera *b)*, è punito con la sanzione amministrativa pecuniaria da euro 200.000 a euro 1.200.000;

b) il mancato adempimento dell'obbligo di notifica di cui al comma 3, lettera *a)*, nei termini prescritti, è punito con la sanzione amministrativa pecuniaria da euro 250.000 a euro 1.500.000;

c) l'inosservanza delle misure di sicurezza di cui al comma 3, lettera *b)*, è punita con la sanzione amministrativa pecuniaria da euro 250.000 a euro 1.500.000;

d) la mancata comunicazione di cui al comma 6, lettera *a)*, nei termini prescritti, è punita con la sanzione amministrativa pecuniaria da euro 300.000 a euro 1.800.000;

e) l'impiego di prodotti e servizi sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici di cui al comma 2, lettera *b)*, in violazione delle condizioni o in assenza del superamento dei test imposti dal CVCN ovvero dai Centri di valutazione di cui al comma 6, lettera *a)*, è punito con la sanzione amministrativa pecuniaria da euro 300.000 a euro 1.800.000;

f) la mancata collaborazione per l'effettuazione delle attività di test di cui al comma 6, lettera *a)*, da parte dei soggetti di cui al medesimo comma 6, lettera *b)*, è punita con la sanzione amministrativa pecuniaria da euro 250.000 a euro 1.500.000;

g) il mancato adempimento delle prescrizioni indicate dal Ministero dello sviluppo economico o dalla Presidenza del Consiglio dei ministri in esito alle attività di ispezione e verifica svolte ai sensi del comma 6, lettera *c)*, è punito con la sanzione amministrativa pecuniaria da euro 250.000 a euro 1.500.000;

h) il mancato rispetto delle prescrizioni di cui al comma 7, lettera *b)*, è punito con la sanzione amministrativa pecuniaria da euro 250.000 a euro 1.500.000.

10. L'impiego di prodotti e di servizi sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici di cui al comma 2, lettera *b)*, in assenza della comunicazione o del superamento dei test o in violazione delle condizioni di cui al comma 6, lettera *a)*, comporta, oltre alle sanzioni di cui al comma 9, lettere *d)* ed *e)*, l'applicazione della sanzione amministrativa accessoria della incapacità ad assumere incarichi di direzione, amministrazione e controllo nelle persone giuridiche e nelle imprese, per un periodo di tre anni a decorrere dalla data di accertamento della violazione.

11. Chiunque, allo scopo di ostacolare o condizionare l'espletamento dei procedimenti di cui al comma 2, lettera *b)*, o al comma 6, lettera *a)*, o delle attività ispettive e di vigilanza previste dal comma 6, lettera *c)*, fornisce informazioni, dati o elementi di fatto non rispondenti al vero, rilevanti per la predisposizione o l'aggiornamento degli elenchi di cui al comma 2, lettera *b)*, o ai fini delle comunicazioni di cui al comma 6, lettera *a)*, o per lo svolgimento delle attività ispettive e di vigilanza di cui al comma 6), lettera *c)* od omette di comunicare entro i termini prescritti i predetti dati, informazioni o elementi di fatto, è punito con la reclusione da uno a tre anni.

11- bis. All'articolo 24-*bis*, comma 3, del decreto legislativo 8 giugno 2001, n. 231, dopo le parole: «di altro ente pubblico,» sono inserite le seguenti: «e dei delitti di cui all'articolo 1, comma 11, del decreto-legge 21 settembre 2019, n. 105,».

12. Le autorità competenti per l'accertamento delle violazioni e per l'irrogazione delle sanzioni amministrative sono la Presidenza del Consiglio dei ministri, per i soggetti pubblici e per i soggetti di cui all'articolo 29 del codice di cui al decreto legislativo 7 marzo 2005, n. 82, di cui al comma 2-*bis*, e il Ministero dello sviluppo economico, per i soggetti privati di cui al medesimo comma.

13. Ai fini dell'accertamento e dell'irrogazione delle sanzioni amministrative di cui al comma 9, si osservano le disposizioni contenute nel capo I, sezioni I e II, della legge 24 novembre 1981, n. 689.

14. Per i dipendenti dei soggetti pubblici di cui al comma 2-*bis*, la violazione delle disposizioni di cui al presente articolo può costituire causa di responsabilità disciplinare e amministrativo-contabile.

15. Le autorità titolari delle attribuzioni di cui al presente decreto assicurano gli opportuni raccordi con il Dipartimento delle informazioni per la sicurezza e con l'organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione, quale autorità di contrasto nell'esercizio delle attività di cui all'articolo 7-*bis* del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155.

16. La Presidenza del Consiglio dei ministri, per lo svolgimento delle funzioni di cui al presente decreto può avvalersi dell'Agenzia per l'Italia Digitale (AgID) sulla base di apposite convenzioni, nell'ambito delle risorse finanziarie e umane disponibili a legislazione vigente, senza nuovi o maggiori oneri per la finanza pubblica.

17. Al decreto legislativo 18 maggio 2018, n. 65, sono apportate le seguenti modificazioni:

a) all'articolo 4, comma 5, dopo il primo periodo è aggiunto il seguente:

«Il Ministero dello sviluppo economico inoltra tale elenco al punto di contatto unico e all'organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione, di cui all'articolo 7-*bis* del decreto- legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155.»;

b) all'articolo 9, comma 3, le parole «e il punto di contatto unico» sono sostituite dalle seguenti:

«, il punto di contatto unico e l'organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione, di cui all'articolo 7-*bis* del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155,».

18. Gli eventuali adeguamenti alle prescrizioni di sicurezza definite ai sensi del presente articolo, delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori pubblici di cui al comma 2-*bis*, sono effettuati con le risorse finanziarie disponibili a legislazione vigente.

19. Per la realizzazione, l'allestimento e il funzionamento del CVCN di cui ai commi 6 e 7 è autorizzata la spesa di euro 3.200.000 per l'anno 2019 e di euro 2.850.000 per ciascuno degli anni dal 2020 al 2023 e di euro 750.000 annui a decorrere dall'anno 2024. Per la realizzazione, l'allestimento e il funzionamento del Centro di valutazione del Ministero dell'interno, di cui ai commi 6 e 7, è autorizzata la spesa di euro 200.000 per l'anno 2019 e di euro 1.500.000 per ciascuno degli anni 2020 e 2021.

19-*bis*. Il Presidente del Consiglio dei ministri coordina la coerente attuazione delle disposizioni del presente decreto che disciplinano il perimetro di sicurezza nazionale cibernetica, anche avvalendosi del Dipartimento delle informazioni per la sicurezza, che assicura gli opportuni raccordi con le autorità titolari delle attribuzioni di cui al presente decreto e con i soggetti di cui al comma 1 del presente articolo. Entro sessanta giorni dalla data di entrata in vigore del regolamento di cui al comma 6, il Presidente del Consiglio dei ministri trasmette alle Camere una relazione sulle attività svolte.

19-*ter*. Nei casi in cui sui decreti del Presidente del Consiglio dei ministri previsti dal presente articolo è acquisito, ai fini della loro adozione, il parere del Consiglio di Stato, i termini ordinatori stabiliti dal presente articolo sono sospesi per un periodo di quarantacinque giorni.»

— Si riporta il testo degli articoli 5 e 10 del decreto del Presidente della Repubblica 15 gennaio 2018, n. 15 «Regolamento a norma dell'articolo 57 del decreto legislativo 30 giugno 2003, n. 196, recante l'individuazione delle modalità di attuazione dei principi del Codice in materia di protezione dei dati personali relativamente al trattamento dei dati effettuato, per le finalità di polizia, da organi, uffici e comandi di polizia»

«Art. 5 *(Configurazione dei sistemi informativi e dei programmi informatici)*. — 1. Ai sensi dell'articolo 3 del Codice, in relazione ai trattamenti automatizzati, i sistemi informativi e i programmi informatici sono configurati in modo da ridurre al minimo l'utilizzo di dati personali e identificativi, escludendone comunque il trattamento quando le finalità di cui all'articolo 3 possono essere perseguite mediante dati anonimi o modalità che consentono di identificare la persona interessata solo in caso di necessità.

2. I nuovi sistemi informativi e programmi informatici sono progettati in modo che i dati personali siano cancellati o resi anonimi, con modalità automatizzate, allo scadere dei termini di conservazione di cui all'articolo 10. Essi, inoltre, sono progettati in modo da consentire la registrazione in appositi registri degli accessi e delle operazioni, di seguito «file di log», effettuati dagli operatori abilitati.»

«Art. 10 *(Termini di conservazione dei dati)*.— 1. I dati personali oggetto di trattamento sono conservati per un periodo di tempo non superiore a quello necessario per il conseguimento delle finalità di polizia di cui all'articolo 3.

2. I dati personali soggetti a trattamento automatizzato, trascorsa la metà del tempo massimo di conservazione di cui al comma 3, se uguale o superiore a quindici anni, sono accessibili ai soli operatori a ciò abilitati e designati, incaricati del trattamento secondo profili di autorizzazione predefiniti in base alle indicazioni del capo dell'ufficio o del comandante del reparto e in relazione a specifiche attività informative, di sicurezza o di indagine di polizia giudiziaria.

3. Fatto salvo quanto previsto dai commi 6 e 7, i dati personali non possono essere conservati oltre il termine massimo fissato come segue:

a) dati relativi a provvedimenti di natura interdittiva, di sicurezza e cautelare, nonché a misure restrittive della libertà personale conseguenti ad una sentenza di condanna - 20 anni dalla cessazione della loro efficacia;

b) dati relativi a misure di prevenzione di carattere personale e patrimoniale - 25 anni dalla cessazione della loro efficacia;

c) dati relativi a procedimenti, misure e provvedimenti su cui interviene una procedura di annullamento, invalidazione o revoca - 3 anni dalla data di inoppugnabilità del provvedimento di annullamento, invalidazione o revoca;

d) dati relativi a provvedimenti che dichiarano l'estinzione della pena o del reato - 8 anni dall'inoppugnabilità del provvedimento;

e) dati derivanti da attività informativa e ispettiva svolta per le finalità di cui all'articolo 3 - 15 anni dall'ultimo trattamento;

f) dati relativi ad attività di polizia giudiziaria conclusa con provvedimento di archiviazione - 20 anni dall'emissione del provvedimento;

g) dati relativi ad attività di polizia giudiziaria conclusa con sentenza di assoluzione o di non doversi procedere — 20 anni dal passaggio in giudicato della sentenza;

h) dati relativi ad attività di polizia giudiziaria conclusa con sentenza di condanna - 25 anni dal passaggio in giudicato della sentenza;

i) dati relativi ad attività di indagine o polizia giudiziaria che non hanno dato luogo a procedimento penale - 15 anni dall'ultimo trattamento;

l) dati relativi ad attività di prevenzione generale e soccorso pubblico - 5 anni dalla raccolta;

m) dati relativi a controlli di polizia - 20 anni dalla raccolta;

n) dati raccolti per l'analisi criminale e di prevenzione — 10 anni dall'elaborazione dell'analisi;

o) dati relativi a provvedimenti di espulsione e rimpatrio di stranieri - 30 anni dall'esecuzione;

p) dati relativi a nulla osta, licenze, autorizzazioni di polizia - 5 anni dalla scadenza o dalla revoca del titolo;

q) dati relativi alla detenzione delle armi o parti di esse, di munizioni finite e di materie esplodenti di qualsiasi genere - 5 anni dalla cessazione della detenzione;

r) dati relativi a persone detenute negli istituti penitenziari - 30 anni dalla scarcerazione a seguito di espiazione della pena in caso di condanna - 5 anni dalla scarcerazione a seguito di decreto di archiviazione o non luogo a procedere o di sentenza di assoluzione;

s) dati relativi a persone sottoposte a misure di sicurezza detentive - 25 anni dalla scadenza del termine di efficacia della misura;

t) dati relativi alla gestione delle attività operative - 10 anni dall'ultimo trattamento;

u) dati raccolti mediante sistemi di ripresa fotografica, audio e video nei servizi di ordine pubblico e di polizia giudiziaria - 3 anni dalla raccolta; dati raccolti mediante sistemi di videosorveglianza o di ripresa fotografica, audio e video di documentazione dell'attività operativa - 18 mesi dalla raccolta. Si applicano i diversi termini di conservazione di cui alla lettera *b)*, quando i dati personali sono confluiti in un procedimento per l'applicazione di una misura di prevenzione, o quelli di cui alle lettere *a)*, *f)*, *g)*, *h)* e *i)*, quando i dati personali sono confluiti in un procedimento penale.

4. I termini di conservazione di cui al comma 3 sono aumentati di due terzi quando i dati personali sono trattati nell'ambito di attività preventiva o repressiva relativa ai delitti di cui all'articolo 51, commi 3-*bis*, 3-*quater* e 3-*quinquies*, del codice di procedura penale, nonché per le ulteriori ipotesi indicate dall'articolo 407, comma 2, lettera *a)*, del codice di procedura penale.

5. Il capo dell'ufficio o il comandante del reparto, prima della scadenza dei termini di cui al comma 3, ove sia strettamente necessario per il conseguimento delle finalità di polizia di cui all'articolo 3, può decidere, sulla base dei criteri definiti dal Capo della polizia - direttore generale della pubblica sicurezza ovvero, su sua delega, dal vice direttore generale di cui all'articolo 4, comma 6, del decreto-legge 29 ottobre 1991, n. 345, convertito, con modificazioni, dalla legge 30 dicembre 1991, n. 410, di aumentare la durata di conservazione, indicandone i motivi in relazione al caso specifico e l'ulteriore periodo di trattamento, che non può comunque superare i due terzi di quelli fissati al comma 3.

6. I dati personali soggetti a trattamento non automatizzato, sono conservati per il periodo di tempo previsto dalle disposizioni sullo scarto dei documenti d'archivio delle pubbliche amministrazioni se superiore a quello di cui al comma 3.

7. Sono fatti salvi i diversi termini e modalità di conservazione dei dati personali previsti da disposizioni di legge o di regolamento, da atti normativi dell'Unione europea o dal diritto internazionale in relazione a specifici trattamenti effettuati per le finalità di cui all'articolo 3.

8. Decorsi i termini di cui ai commi 1, 3, 4, 5 e 7, i dati personali soggetti a trattamento automatizzato sono cancellati o resi anonimi, i dati personali non soggetti a trattamento automatizzato restano assoggettati alle disposizioni sullo scarto dei documenti d'archivio delle pubbliche amministrazioni.».

— Si riporta il testo dell'articolo 53, comma 3, del decreto legislativo 30 giugno 2003, n. 196 «Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e

del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE»:

«Art. 53 *(Ambito applicativo e titolari dei trattamenti)*. — Omissis

3. Con decreto adottato dal Ministro dell'interno, previa comunicazione alle competenti Commissioni parlamentari, sono individuati, nell'allegato *C)* al presente codice, i trattamenti non occasionali di cui al comma 2 effettuati con strumenti elettronici e i relativi titolari.»

— Il decreto del Presidente del Consiglio dei ministri del 14 aprile 2021, n. 81 recante «Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'articolo 1, comma 2, lettera *b)*, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e di misure volte a garantire elevati livelli di sicurezza» è pubblicato nella Gazz. Uff. 11 giugno 2021, n. 138.

Note all'art. 1:

— Si riporta il testo dell'art. 11, del citato decreto legislativo 10 agosto 2018, n. 104:

«Art. 11 *(Norme di semplificazione in materia di tracciabilità delle armi e delle munizioni)*. — 1. Al fine di assicurare standard uniformi degli strumenti di controllo delle armi da fuoco e delle munizioni e garantire lo scambio di dati con gli altri Stati membri dell'Unione europea, è istituito presso il Dipartimento della Pubblica Sicurezza, un sistema informatico dedicato per la tracciabilità delle armi e delle munizioni.

2. Il sistema di cui al comma 1 contiene le seguenti informazioni:

a) per le armi da fuoco il tipo, la marca, il modello, il calibro, il numero di catalogo se presente, la classificazione secondo la normativa europea se presente, il numero di matricola di ciascuna arma e la marcatura apposta sul telaio o sul fusto quale marcatura unica ai sensi dell'articolo 11 della legge 18 aprile 1975, n. 110, nonché il numero di matricola o la marcatura unica applicata alle loro parti, nel caso in cui questa differisca dalla marcatura apposta sul telaio o sul fusto di ciascuna arma da fuoco. Il sistema contiene, altresì, i dati identificativi dei fornitori, degli acquirenti, dei detentori dell'arma, ivi compresi quelli riguardanti la sede legale qualora tali soggetti esercitino attività d'impresa, l'indicazione delle operazioni aventi ad oggetto ogni arma e la data in cui sono state effettuate, il relativo prezzo, nonché gli estremi del titolo abilitativo all'acquisto e, nel caso di persona fisica diversa dall'imprenditore, il luogo di residenza. Nel sistema sono, inoltre, inseriti i dati relativi a qualsiasi operazione consistente in una trasformazione o modifica irreversibile dell'arma da fuoco che determini un cambiamento della categoria o della sottocategoria di cui all'allegato I alla direttiva 91/477/CEE del Consiglio, del 18 giugno 1991, incluse la disattivazione o la distruzione certificate e la data in cui sono avvenute tali operazioni;

b) per le munizioni, le informazioni previste dall'articolo 55, primo comma, del regio decreto 18 giugno 1931, n. 773 e i dati di cui all'articolo 3, comma 2, lettere *a)*, *b)* e *c)*, della legge 6 dicembre 1993, n. 509;

c) per le armi diverse dalle armi da fuoco, le informazioni previste dall'articolo 35 del regio decreto 18 giugno 1931, n. 773 e dall'articolo 54, primo comma, del regio decreto 6 maggio 1940, n. 635, ivi compresi i dati relativi alle armi a modesta capacità offensiva.

3. I soggetti tenuti alla conservazione dei registri di cui all'articolo 35 e, limitatamente alle munizioni, all'articolo 55 del testo unico delle leggi di pubblica sicurezza, di cui al regio decreto 18 giugno 1931, n. 773, provvedono ad immettere i dati relativi alle operazioni eseguite, secondo le modalità stabilite con i provvedimenti di cui al comma 6. L'inserimento dei dati nel sistema di cui al comma 1 costituisce valida modalità di assolvimento degli obblighi di cui all'articolo 35 e, limitatamente alle munizioni all'articolo 55 del testo unico delle leggi di pubblica sicurezza, di cui al regio decreto 18 giugno 1931, n. 773.

4. I dati concernenti le operazioni relative alle armi compiute dagli acquirenti e detentori diversi dai soggetti di cui al comma 3, sono inseriti dall'ufficio locale di pubblica sicurezza o, quando questo manchi, dal locale comando dell'Arma dei Carabinieri ovvero dalla Questura competente per territorio in caso di trasmissione della denuncia per via telematica.

5. Il sistema informatico è consultabile dal personale delle Forze di polizia di cui all'articolo 16, primo comma, della legge 1° aprile 1981, n. 121, nonché dal personale dell'Amministrazione civile dell'interno, in servizio presso le Prefetture - Uffici Territoriali del Governo, le Questure e gli uffici locali di pubblica sicurezza, per le finalità di controllo della circolazione delle armi e delle munizioni, nonché per la prevenzione e repressione dei reati commessi a mezzo di essi.

6. Con decreto del Ministro dell'interno adottato ai sensi dell'articolo 17, comma 3, della legge 23 agosto 1988, n. 400, di concerto con il Ministro dell'economia e delle finanze, sentiti il Ministero della difesa e il Garante per la protezione dei dati personali, sono disciplinate, in conformità alle vigenti disposizioni in materia di tutela dei dati personali in ambito giudiziario e per finalità di polizia, le modalità:

a) di funzionamento del sistema informatico;

b) di trasmissione e conservazione dei dati previsti dall'articolo 35 e, limitatamente alle munizioni, dall'articolo 55 del testo unico delle leggi di pubblica sicurezza, di cui al regio decreto 18 giugno 1931, n. 773;

c) di autenticazione, autorizzazione e registrazione degli accessi e delle operazioni effettuate sul sistema;

d) di collegamento, ai fini di consultazione e riscontro dei dati, con il Centro elaborazione dati di cui all'articolo 8 della legge 1° aprile 1981, n. 121;

e) di verifica della qualità e protezione dal danneggiamento e dalla distruzione accidentale o dolosa dei dati registrati e la loro sicura conservazione;

f) di trasmissione delle informazioni qualora il sistema informatico di cui al comma 1 non sia in grado di funzionare regolarmente a causa di eventi eccezionali.

7. Gli oneri derivanti dall'attuazione del presente articolo sono pari a euro 500.000 per l'anno 2018 e ad euro 1.000.000 per l'anno 2019, per l'istituzione del sistema informatico, e ad euro 300.000 annui a decorrere dall'anno 2020, per le attività di gestione e manutenzione del sistema.»

— Per il testo dell'articolo 1-*bis*, comma 1, lett. *f)* e *g)* del decreto legislativo 30 dicembre 1992, n. 527, v. nelle note alle premesse.

— Si riporta il testo dell'articolo 31-*bis*, del citato regio decreto 18 giugno 1931, n. 773:

«Art. 31-bis

1. Fatte salve le previsioni di cui agli articoli 01, comma 1, lettera *p)*, e 1, comma 11, della legge 9 luglio 1990, n. 185, come modificata dal decreto legislativo 22 giugno 2012, n. 105, per esercitare l'attività di intermediario di cui all'articolo 1-*bis*, comma 1, lettera *f)*, del decreto legislativo 30 dicembre 1992, n. 527, nel settore delle armi, è richiesta una apposita licenza rilasciata dal questore, che ha una validità di 3 anni. Si applicano in quanto compatibili le disposizioni anche regolamentari previste per la licenza di cui all'articolo 31. La licenza non è necessaria per i rappresentanti in possesso di mandato delle parti interessate. Del mandato è data comunicazione alla Questura competente per territorio.

2. Ogni operatore autorizzato deve comunicare, l'ultimo giorno del mese, all'autorità che ha rilasciato la licenza un resoconto dettagliato delle singole operazioni effettuate nel corso dello stesso mese. Il resoconto può essere trasmesso anche all'indirizzo di posta elettronica certificata della medesima autorità. L'operatore, nel caso in cui abbia la materiale disponibilità delle armi o delle munizioni, è obbligato alla tenuta del registro di cui, rispettivamente, agli articoli 35 e 55, nonché ad effettuare le relative annotazioni concernenti le operazioni eseguite.

3. La mancata comunicazione può comportare, in caso di prima violazione, la sospensione e, in caso di recidiva, la sospensione o la revoca della licenza.»

— Per il testo degli articoli 35 e 55 del regio decreto 18 giugno 1931, n. 773, v. nelle note alle premesse.

— Per il testo dell'articolo 8 della legge 1° aprile 1981, n. 121, v. nelle note alle premesse.

Note all'art. 2:

— Si riporta il testo dell'articolo 1-*bis*, comma 1, lettera *a)*, *b)* e *d)* del citato decreto legislativo 30 dicembre 1992, n. 527:

«Art. 1-*bis*. 1. Ai fini del presente decreto, si intende per:

a) «arma da fuoco», qualsiasi arma portatile a canna che espelle, è progettata per espellere o può essere trasformata al fine di espellere un colpo, una pallottola o un proiettile mediante l'azione di un propellente

combustibile, ad eccezione degli oggetti di cui al punto III dell'allegato I della direttiva 91/477/CEE, e successive modificazioni. Si considera, altresì, "arma da fuoco" qualsiasi oggetto idoneo a essere trasformato al fine di espellere un colpo, una pallottola o un proiettile mediante l'azione di un propellente combustibile se:

1) ha l'aspetto di un'arma da fuoco e,

2) come risultato delle sue caratteristiche di fabbricazione o del materiale a tal fine utilizzato, può essere così trasformato;

b) «parte», ciascuna delle seguenti componenti essenziali: la canna, il telaio, il fusto, comprese le parti sia superiore sia inferiore (*upper receiver e lower receiver*), nonché, in relazione alle modalità di funzionamento, il carrello, il tamburo, l'otturatore o il blocco di culatta che, in quanto oggetti distinti, rientrano nella categoria in cui è stata classificata l'arma da fuoco sulla quale sono installati o sono destinati ad essere installati;

omissis

d) «munizione», l'insieme della cartuccia o dei suoi componenti, compresi i bossoli, gli inneschi, la polvere da sparo, le pallottole o i proiettili, utilizzati in un'arma da fuoco a condizione che tali componenti siano soggetti ad autorizzazione;

omissis.»

— Per il testo dell'articolo 1-*bis*, comma 1, lett. *f)* e *g)* del decreto legislativo 30 dicembre 1992, n. 527, v. nelle note alle premesse.

— Si riporta il testo degli articoli 10, settimo comma e 22, primo comma, della citata legge 18 aprile 1975, n. 110:

«Art. 10 *(Divieto di detenzione e raccolta di armi da guerra. Collezione di armi comuni da sparo)*. — Omissis

7. Restano ferme le disposizioni del testo unico delle leggi di pubblica sicurezza 18 giugno 1931, n. 773, per le armi antiche. Sono armi antiche quelle ad avancarica e quelle fabbricate anteriormente al 1890. Per le armi antiche, artistiche o rare di importanza storica di modelli anteriori al 1890 sarà disposto un apposito regolamento da emanarsi di concerto tra il Ministro per l'interno e il Ministro per i beni culturali entro sei mesi dall'entrata in vigore della presente legge. Dette armi non si computano ai fini di cui al sesto comma.

Omissis.»

«Art. 22 *(Locazione e comodato di armi)*. — 1. Non è consentita la locazione o il comodato delle armi di cui agli articoli 1 e 2, salvo che si tratti di armi per uso scenico, ovvero di armi destinate ad uso sportivo o di caccia, ovvero che il conduttore o accomodatario sia munito di autorizzazione per la fabbricazione di armi o munizioni ed il contratto avvenga per esigenze di studio, di esperimento, di collaudo. Per armi da fuoco per uso scenico si intendono le armi alle quali, con semplici accorgimenti tecnici, venga occlusa parzialmente la canna al solo scopo di impedire che possa espellere un proiettile ed il cui impiego avvenga costantemente sotto il controllo dell'armaiolo che le ha in carico. Le armi da fuoco per uso scenico sono sottoposte, a spese dell'interessato, a verifica del Banco nazionale di prova, che vi apporrà specifico punzone.

Omissis.».

— Per il testo dell'articolo 8 della legge 1° aprile 1981, n. 121, v. nelle note alle premesse.

— Si riporta il testo dell'articolo 108 del decreto legislativo 6 settembre 2011, n. 159 (Codice delle leggi antimafia e delle misure di prevenzione, nonché nuove disposizioni in materia di documentazione antimafia, a norma degli articoli 1 e 2 della legge 13 agosto 2010, n. 136):

«Art. 108 *(Direzione investigativa antimafia)*. — 1. È istituita, nell'ambito del Dipartimento della pubblica sicurezza, una Direzione investigativa antimafia (D.I.A.) con il compito di assicurare lo svolgimento, in forma coordinata, delle attività di investigazione preventiva attinenti alla criminalità organizzata, nonché di effettuare indagini di polizia giudiziaria relative esclusivamente a delitti di associazione di tipo mafioso o comunque ricollegabili all'associazione medesima.

2. Formano oggetto delle attività di investigazione preventiva della Direzione investigativa antimafia le connotazioni strutturali, le articolazioni e i collegamenti interni ed internazionali delle organizzazioni criminali, gli obiettivi e le modalità operative di dette organizzazioni, nonché ogni altra forma di manifestazione delittuosa alle stesse riconducibile ivi compreso il fenomeno delle estorsioni.

3. La Direzione investigativa antimafia nell'assolvimento dei suoi compiti opera in stretto collegamento con gli uffici e le strutture delle forze di polizia esistenti a livello centrale e periferico.

4. Tutti gli ufficiali ed agenti di polizia giudiziaria debbono fornire ogni possibile cooperazione al personale investigativo della D.I.A. Gli ufficiali ed agenti di polizia giudiziaria dei servizi centrali e interprovinciali di cui all'articolo 12 del decreto-legge 13 maggio 1991, n. 152, convertito in legge 12 luglio 1991, n. 203, devono costantemente informare il personale investigativo della D.I.A., incaricato di effettuare indagini collegate, di tutti gli elementi informativi ed investigativi di cui siano venuti comunque in possesso e sono tenuti a svolgere, congiuntamente con il predetto personale, gli accertamenti e le attività investigative eventualmente richiesti. Il predetto personale dei servizi centrali e interprovinciali della Polizia di Stato, dell'Arma dei carabinieri e del Corpo della guardia di finanza, a decorrere dal 1° gennaio 1993, è assegnato alla D.I.A., nei contingenti e con i criteri e le modalità determinati con decreto del Ministro dell'interno, di concerto con i Ministri della difesa e delle finanze.

5. Al Direttore della Direzione Investigativa Antimafia è attribuita la responsabilità generale delle attività svolte dalla D.I.A., delle quali riferisce periodicamente al Consiglio generale di cui all'articolo 107, e competono i provvedimenti occorrenti per l'attuazione, da parte della D.I.A., delle direttive emanate a norma del medesimo articolo 107.

6. Alla D.I.A. è preposto un direttore tecnico-operativo scelto fra funzionari appartenenti ai ruoli della Polizia di Stato, con qualifica non inferiore a dirigente superiore, e ufficiali di grado non inferiore a generale di brigata dell'Arma dei carabinieri e del Corpo della guardia di finanza, che abbiano maturato specifica esperienza nel settore della lotta alla criminalità organizzata. Il direttore della D.I.A. riferisce al Consiglio generale di cui all'articolo 107 sul funzionamento dei servizi posti alle sue dipendenze e sui risultati conseguiti.

7. Con gli stessi criteri indicati al comma 6 è assegnato alla D.I.A. un vice direttore con funzioni vicarie.

8. La D.I.A. si avvale di personale dei ruoli della Polizia di Stato, dell'Arma dei carabinieri e del Corpo della guardia di finanza, nonché del Corpo di polizia penitenziaria e del Corpo forestale dello Stato. Il personale dei ruoli del Corpo di polizia penitenziaria e del Corpo forestale dello Stato opera nell'ambito delle articolazioni centrali e periferiche della D.I.A. per le esigenze di collegamento con le strutture di appartenenza, anche in relazione a quanto previsto dal comma 3, nonché per l'attività di analisi sullo scambio delle informazioni di interesse all'interno delle strutture carcerarie e di quelle connesse al contrasto delle attività organizzate per il traffico illecito di rifiuti e agli altri compiti di istituto. Con decreto del Ministro dell'interno, di concerto con i Ministri della giustizia, delle politiche agricole alimentari e forestali e dell'economia e delle finanze sono definiti i contingenti di personale del Corpo di polizia penitenziaria e del Corpo forestale dello Stato che opera nell'ambito della D.I.A., nonché le modalità attuative di individuazione, di assegnazione e di impiego del medesimo personale.

9. Il Ministro dell'interno, sentito il Consiglio generale di cui all'articolo 107, determina l'organizzazione della D.I.A. secondo moduli rispondenti alla diversificazione dei settori d'investigazione e alla specificità degli ordinamenti delle forze di polizia interessate, fermo restando che in ogni caso, nella prima fase, l'organizzazione è articolata come segue:

a) reparto investigazioni preventive;

b) reparto investigazioni giudiziarie;

c) reparto relazioni internazionali ai fini investigativi.

10. Alla determinazione del numero e delle competenze delle divisioni in cui si articolano i reparti di cui al comma 9 si provvede con le modalità e procedure indicate nell'articolo 5, settimo comma, della legge 1° aprile 1981, n. 121, e successive modificazioni e integrazioni. Con le stesse modalità e procedure si provvede alla preposizione ed assegnazione del personale ai reparti e alle divisioni, secondo principi di competenza tecnico-professionale e con l'obiettivo di realizzare nei confronti dei titolari degli uffici predetti di pari livello una sostanziale parità ed equiordinazione di funzioni, anche mediante il ricorso al criterio della rotazione degli incarichi.»

— Per il decreto legislativo 18 maggio 2018, n. 51, v. nelle note alle premesse

— Per il decreto legislativo 10 agosto 2018, n. 104, v. nelle note alle premesse.

— Si riporta il testo degli articoli 4 e 16, comma 1, della citata legge 1° aprile 1981, n. 121:

«Art. 4 *(Dipartimento della pubblica sicurezza)*. — Nell'ambito dell'Amministrazione della pubblica sicurezza è istituito il dipartimento della pubblica sicurezza che provvede, secondo le direttive e gli ordini del Ministro dell'interno:

1) all'attuazione della politica dell'ordine e della sicurezza pubblica;

2) al coordinamento tecnico-operativo delle forze di polizia;

3) alla direzione e amministrazione della Polizia di Stato;

4) alla direzione e gestione dei supporti tecnici, anche per le esigenze generali del Ministero dell'interno.»

«Art. 16 *(Forze di polizia)*. — Ai fini della tutela dell'ordine e della sicurezza pubblica, oltre alla polizia di Stato sono forze di polizia, fermi restando i rispettivi ordinamenti e dipendenze:

a) l'Arma dei carabinieri, quale forza armata in servizio permanente di pubblica sicurezza;

b) il Corpo della guardia di finanza, per il concorso al mantenimento dell'ordine e della sicurezza pubblica.

Omissis.».

— Si riporta il testo dell'articolo 8, secondo comma, del citato regio decreto 18 giugno 1931, n. 773:

«Art. 8

Omissis

Nei casi in cui è consentita la rappresentanza nell'esercizio di una autorizzazione di polizia, il rappresentante deve possedere i requisiti necessari per conseguire l'autorizzazione e ottenere l'approvazione dell'autorità di pubblica sicurezza che ha conceduta l'autorizzazione.»

— Per il regolamento delegato (UE) 2019/686, vedasi nelle note alle premesse.

— Si riporta il testo dell'articolo 12 del decreto ministeriale 9 agosto 2001, n. 362: «Regolamento recante la disciplina specifica dell'utilizzo delle armi ad aria compressa o a gas compressi, sia lunghe che corte, i cui proiettili erogano un'energia cinetica non superiore a 7,5 joule e delle repliche di armi antiche ad avancarica di modello anteriore al 1890 a colpo singolo»:

«Art. 12 (*Definizione)*. — 1. Le repliche di armi antiche ad avancarica a colpo singolo di modello e/o tipologia anteriore al 1890 utilizzano per il funzionamento a fuoco munizionamento costituito da polvere nera, od equivalente, palla o pallini di piombo, che vengono introdotti singolarmente nella canna dalla volata o dalla parte anteriore della camera di scoppio; esse sono dotate di un sistema di accensione a miccia e/o a pietra e/o a capsula e sono portatili.»

— Per il testo dell'articolo 11, del decreto legislativo 10 agosto 2018, n. 104, v. nelle note all'art. 1.

— Si riporta il testo dell'art. 3 del citato decreto legislativo 18 maggio 2018, n. 51:

«Art. 3. *(Principi applicabili al trattamento di dati personali)*. — 1. I dati personali di cui all'articolo 1, comma 2, sono:

a) trattati in modo lecito e corretto;

b) raccolti per finalità determinate, espresse e legittime e trattati in modo compatibile con tali finalità;

c) adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali sono trattati;

d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;

e) conservati con modalità che consentano l'identificazione degli interessati per il tempo necessario al conseguimento delle finalità per le quali sono trattati, sottoposti a esame periodico per verificarne la persistente necessità di conservazione, cancellati o anonimizzati una volta decorso tale termine;

f) trattati in modo da garantire un'adeguata sicurezza e protezione da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali, mediante l'adozione di misure tecniche e organizzative adeguate.

2. Il trattamento per una delle finalità di cui all'articolo 1, comma 2, diversa da quella per cui i dati sono raccolti, è consentito se il titolare del trattamento, anche se diverso da quello che ha raccolto i dati, è autorizzato a trattarli per detta finalità, conformemente al diritto dell'Unione europea o dell'ordinamento interno e se il trattamento è necessario e proporzionato a tale diversa finalità, conformemente al diritto dell'Unione europea o dell'ordinamento interno.

3. Il trattamento per le finalità di cui all'articolo 1, comma 2, può comprendere l'archiviazione nel pubblico interesse, l'utilizzo scientifico, storico o statistico, fatte salve le garanzie adeguate per i diritti e le libertà degli interessati.

4. Il titolare del trattamento è responsabile del rispetto dei principi di cui ai commi 1, 2 e 3.»

— Si riporta il testo dell'articolo 4, comma 2, lett. *g)* del decreto del Presidente del Consiglio dei Ministri 11 giugno 2019, n. 78 (Regolamento recante l'organizzazione degli Uffici centrali di livello dirigenziale generale del Ministero dell'interno):

«Art. 4 *(Dipartimento della pubblica sicurezza)*. — *Omissis*.

2. Il Dipartimento della pubblica sicurezza è articolato, secondo i criteri di organizzazione e le modalità stabiliti dalla legge 1° aprile 1981, n. 121 e in armonia con i princìpi generali dell'ordinamento ministeriale, nelle seguenti direzioni centrali e uffici di pari livello anche a carattere interforze:

Omissis.

g) Direzione centrale della polizia criminale: supporto per l'esercizio delle funzioni demandate al vice direttore generale della pubblica sicurezza - Direttore centrale della polizia criminale anche ai fini dei compiti di collegamento tra la Direzione investigativa antimafia e gli altri uffici e strutture di cui all'articolo 4, comma 6, del decreto-legge 29 ottobre 1991, n. 345, convertito, con modificazioni, dalla legge 30 dicembre 1991, n. 410; raccolta, classificazione e analisi delle informazioni e dei dati, a carattere interforze, in materia di tutela dell'ordine e della sicurezza pubblica, nonché di contrasto delle fenomenologie criminali più rilevanti; espletamento, in attuazione della pianificazione strategica delle relazioni internazionali, dei compiti di cooperazione di polizia a livello europeo ed internazionale, salvo quanto previsto alla lettera *n)*; gestione dei collaboratori e testimoni di giustizia; gestione del CED Interforze di cui all'articolo 8 della legge n. 121 del 1981, per l'attuazione dell'interoperabilità tra i sistemi informatici delle Forze di polizia, anche mediante la standardizzazione delle metodologie di comunicazione, nel rispetto delle normative in materia di protezione e sicurezza dei dati personali;

Omissis.»

— Si riporta il testo dell'articolo 1 del decreto legislativo 7 marzo 2005, n. 82 (Codice dell'amministrazione digitale):

«Art. 1 *(Definizioni)*. — 1. Ai fini del presente codice si intende per:

0a) AgID: l'Agenzia per l'Italia digitale di cui all'articolo 19 del decreto-legge 22 giugno 2012, n. 83, convertito, con modificazioni, dalla legge 7 agosto 2012, n. 134;

[a) allineamento dei dati: il processo di coordinamento dei dati presenti in più archivi finalizzato alla verifica della corrispondenza delle informazioni in essi contenute;

[b) autenticazione del documento informatico: la validazione del documento informatico attraverso l'associazione di dati informatici relativi all'autore o alle circostanze, anche temporali, della redazione;

c) carta d'identità elettronica: il documento d'identità munito di elementi per l'identificazione fisica del titolare rilasciato su supporto informatico dalle amministrazioni comunali con la prevalente finalità di dimostrare l'identità anagrafica del suo titolare;

d) carta nazionale dei servizi: il documento rilasciato su supporto informatico per consentire l'accesso per via telematica ai servizi erogati dalle pubbliche amministrazioni;

[e) certificati elettronici: gli attestati elettronici che collegano all'identità del titolare i dati utilizzati per verificare le firme elettroniche;

[f) certificato qualificato: il certificato elettronico conforme ai requisiti di cui all'allegato I della direttiva 1999/93/CE, rilasciati da certificatori che rispondono ai requisiti di cui all'allegato II della medesima direttiva;

[g) certificatore: il soggetto che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime;

[h) chiave privata: l'elemento della coppia di chiavi asimmetriche, utilizzato dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico;

([i) chiave pubblica: l'elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento informatico dal titolare delle chiavi asimmetriche;

i-*bis*) copia informatica di documento analogico: il documento informatico avente contenuto identico a quello del documento analogico da cui è tratto;

i-*ter*) copia per immagine su supporto informatico di documento analogico: il documento informatico avente contenuto e forma identici a quelli del documento analogico da cui è tratto;

i-*quater*) copia informatica di documento informatico: il documento informatico avente contenuto identico a quello del documento da cui è tratto su supporto informatico con diversa sequenza di valori binari;

i-*quinquies*) duplicato informatico: il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario;

i-*sexies*) dati territoriali: i dati che attengono, direttamente o indirettamente, a una località o a un'area geografica specifica;

[l) dato a conoscibilità limitata: il dato la cui conoscibilità è riservata per legge o regolamento a specifici soggetti o categorie di soggetti;

l-*bis*) formato aperto: un formato di dati reso pubblico, documentato esaustivamente e neutro rispetto agli strumenti tecnologici necessari per la fruizione dei dati stessi;

l-*ter*) dati di tipo aperto: i dati che presentano le seguenti caratteristiche: 1) sono disponibili secondo i termini di una licenza o di una previsione normativa che ne permetta l'utilizzo da parte di chiunque, anche per finalità commerciali, in formato disaggregato; 2) sono accessibili attraverso le tecnologie dell'informazione e della comunicazione, ivi comprese le reti telematiche pubbliche e private, in formati aperti ai sensi della lettera l-*bis*), sono adatti all'utilizzo automatico da parte di programmi per elaboratori e sono provvisti dei relativi metadati; 3) sono resi disponibili gratuitamente attraverso le tecnologie dell'informazione e della comunicazione, ivi comprese le reti telematiche pubbliche e private, oppure sono resi disponibili ai costi marginali sostenuti per la loro riproduzione e divulgazione salvo quanto previsto dall'articolo 7 del decreto legislativo 24 gennaio 2006, n. 36;

m) - n);

n-*bis*) riutilizzo: uso del dato di cui all'articolo 2, comma 1, lettera *e)*, del decreto legislativo 24 gennaio 2006, n. 36;

n-*ter*) domicilio digitale: un indirizzo elettronico eletto presso un servizio di posta elettronica certificata o un servizio elettronico di recapito certificato qualificato, come definito dal regolamento (UE) 23 luglio 2014 n. 910 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE, di seguito «Regolamento eIDAS»,valido ai fini delle comunicazioni elettroniche aventi valore legale;

n-*quater*) servizio in rete o on-line: qualsiasi servizio di una amministrazione pubblica fruibile a distanza per via elettronica;

o);

p) documento informatico: il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti;

p-*bis*) documento analogico: la rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti;

q) - r);

s) firma digitale: un particolare tipo di firma qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare di firma elettronica tramite la chiave privata e a un soggetto terzo tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici;

t) - u);

u-*bis*) gestore di posta elettronica certificata: il soggetto che presta servizi di trasmissione dei documenti informatici mediante la posta elettronica certificata;

u-*ter*);

u-*quater*) identità digitale: la rappresentazione informatica della corrispondenza tra un utente e i suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale secondo le modalità fissate nel decreto attuativo dell'articolo 64;

v) originali non unici: i documenti per i quali sia possibile risalire al loro contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi;

v-*bis*) posta elettronica certificata: sistema di comunicazione in grado di attestare l'invio e l'avvenuta consegna di un messaggio di posta elettronica e di fornire ricevute opponibili ai terzi;

z);

aa) titolare di firma elettronica: la persona fisica cui è attribuita la firma elettronica e che ha accesso ai dispositivi per la sua creazione nonché alle applicazioni per la sua apposizione della firma elettronica;

bb);

cc) titolare del dato: uno dei soggetti di cui all'articolo 2, comma 2, che ha originariamente formato per uso proprio o commissionato ad altro soggetto il documento che rappresenta il dato, o che ne ha la disponibilità;

dd) interoperabilità: caratteristica di un sistema informativo, le cui interfacce sono pubbliche e aperte, di interagire in maniera automatica con altri sistemi informativi per lo scambio di informazioni e l'erogazione di servizi;

ee) cooperazione applicativa: la parte del Sistema Pubblico di Connettività finalizzata all'interazione tra i sistemi informatici dei soggetti partecipanti, per garantire l'integrazione dei metadati, delle informazioni, dei processi e procedimenti amministrativi;

ff) Linee guida: le regole tecniche e di indirizzo adottate secondo il procedimento di cui all'articolo 71.

1-*bis*. Ai fini del presente Codice, valgono le definizioni di cui all'articolo 3 del Regolamento eIDAS.

1-*ter*. Ove la legge consente l'utilizzo della posta elettronica certificata è ammesso anche l'utilizzo di altro servizio elettronico di recapito certificato qualificato ai sensi degli articoli 3, numero 37), e 44 del Regolamento eIDAS.»

— Per il Regolamento UE n. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014, v. nelle note alle premesse.

— Si riporta il testo dell'art. 64 del citato decreto legislativo 7 marzo 2005, n. 82:

«Art. 64 *(Sistema pubblico per la gestione delle identità digitali e modalità di accesso ai servizi erogati in rete dalle pubbliche amministrazioni).* —1. - 2.

2-*bis*. Per favorire la diffusione di servizi in rete e agevolare l'accesso agli stessi da parte di cittadini e imprese, anche in mobilità, è istituito, a cura dell'Agenzia per l'Italia digitale, il sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID).

2-*ter*. Il sistema SPID è costituito come insieme aperto di soggetti pubblici e privati che, previo accreditamento da parte dell'AgID, secondo modalità definite con il decreto di cui al comma 2-*sexies*, identificano gli utenti per consentire loro il compimento di attività e l'accesso ai servizi in rete.

2-*quater*. L'accesso ai servizi in rete erogati dalle pubbliche amministrazioni che richiedono identificazione informatica avviene tramite SPID, nonché tramite la carta di identità elettronica. Il sistema SPID è adottato dalle pubbliche amministrazioni nei tempi e secondo le modalità definiti con il decreto di cui al comma 2-*sexies*. Resta fermo quanto previsto dall'articolo 3-*bis*, comma 01.

2-*quinquies*. Ai fini dell'erogazione dei propri servizi in rete, è altresì riconosciuta ai soggetti privati, secondo le modalità definite con il decreto di cui al comma 2-*sexies*, la facoltà di avvalersi del sistema SPID per la gestione dell'identità digitale dei propri utenti, nonché la facoltà di avvalersi della carta di identità elettronica. L'adesione al sistema SPID ovvero l'utilizzo della carta di identità elettronica per la verifica dell'accesso ai propri servizi erogati in rete per i quali è richiesto il riconoscimento dell'utente esonera i predetti soggetti da un obbligo generale di sorveglianza delle attività sui propri siti, ai sensi dell'articolo 17 del decreto legislativo 9 aprile 2003, n. 70.

2-*sexies*. Con decreto del Presidente del Consiglio dei ministri, su proposta del Ministro delegato per l'innovazione tecnologica e del Ministro per la pubblica amministrazione e la semplificazione, di concerto con il Ministro dell'economia e delle finanze, sentito il Garante per la protezione dei dati personali, sono definite le caratteristiche del sistema SPID, anche con riferimento:

a) al modello architetturale e organizzativo del sistema;

b) alle modalità e ai requisiti necessari per l'accreditamento dei gestori dell'identità digitale;

c) agli standard tecnologici e alle soluzioni tecniche e organizzative da adottare anche al fine di garantire l'interoperabilità delle credenziali e degli strumenti di accesso resi disponibili dai gestori dell'identità digitale nei riguardi di cittadini e imprese;

d) alle modalità di adesione da parte di cittadini e imprese in qualità di utenti di servizi in rete;

e) ai tempi e alle modalità di adozione da parte delle pubbliche amministrazioni in qualità di erogatori di servizi in rete;

f) alle modalità di adesione da parte delle imprese interessate in qualità di erogatori di servizi in rete.

2-*septies*. - 2-*octies*.

2-*nonies*. L'accesso di cui al comma 2-*quater* può avvenire anche con la carta nazionale dei servizi.

2-*decies*. Le pubbliche amministrazioni, in qualità di fornitori dei servizi, usufruiscono gratuitamente delle verifiche rese disponibili dai gestori di identità digitali e dai gestori di attributi qualificati.

2-*undecies*. I gestori dell'identità digitale accreditati sono iscritti in un apposito elenco pubblico, tenuto da AGID, consultabile anche in via telematica.

2-*duodecies*. La verifica dell'identità digitale con livello di garanzia almeno significativo, ai sensi dell'articolo 8, paragrafo 2, del Regolamento (UE) n. 910/2014 del Parlamento e del Consiglio europeo del 23 luglio 2014, produce, nelle transazioni elettroniche o per l'accesso ai servizi in rete, gli effetti del documento di riconoscimento equipollente, di cui all'articolo 35 del testo unico di cui al decreto del Presidente della Repubblica 28 dicembre 2000, n. 445. La disposizione di cui al periodo precedente si applica altresì in caso di identificazione elettronica ai fini dell'accesso ai servizi erogati dalle pubbliche amministrazioni e dai soggetti privati tramite canali fisici. L'identità digitale, verificata ai sensi del presente articolo e con livello di sicurezza almeno significativo, attesta gli attributi qualificati dell'utente, ivi compresi i dati relativi al possesso di abilitazioni o autorizzazioni richieste dalla legge ovvero stati, qualità personali e fatti contenuti in albi, elenchi o registri pubblici o comunque accertati da soggetti titolari di funzioni pubbliche, ovvero gli altri dati, fatti e informazioni funzionali alla fruizione di un servizio attestati da un gestore di attributi qualificati, secondo le modalità stabilite da AGID con Linee guida.

3.

3-*bis*. Fatto salvo quanto previsto dal comma 2-*nonies*, i soggetti di cui all'articolo 2, comma 2, lettera *a)*, utilizzano esclusivamente le identità digitali SPID e la carta di identità elettronica ai fini dell'identificazione dei cittadini che accedono ai propri servizi in rete. Con uno o più decreti del Presidente del Consiglio dei ministri o del Ministro delegato per l'innovazione tecnologica e la transizione digitale è stabilita la data a decorrere dalla quale i soggetti di cui all'articolo 2, comma 2, lettera *a)*, utilizzano esclusivamente le identità digitali SPID, la carta di identità elettronica e la Carta Nazionale dei servizi per consentire l'accesso delle imprese e dei professionisti ai propri servizi in rete, nonché la data a decorrere dalla quale i soggetti di cui all'articolo 2, comma 2, lettere *b)* e *c)* utilizzano esclusivamente le identità digitali SPID, la carta di identità elettronica e la carta Nazionale dei servizi ai fini dell'identificazione degli utenti dei propri servizi on-line.

3-*ter*. I gestori dell'identità digitale accreditati, in qualità di gestori di pubblico servizio, prima del rilascio dell'identità digitale a una persona fisica, verificano i dati identificativi del richiedente, ivi inclusi l'indirizzo di residenza e, ove disponibili, il domicilio digitale o altro indirizzo di contatto, mediante consultazione gratuita dei dati disponibili presso l'ANPR di cui all'articolo 62, anche tramite la piattaforma prevista dall'articolo 50-*ter*. Tali verifiche sono svolte anche successivamente al rilascio dell'identità digitale, con cadenza almeno annuale, anche ai fini della verifica dell'esistenza in vita. Il direttore dell'AGID, previo accertamento dell'operatività delle funzionalità necessarie, fissa la data a decorrere dalla quale i gestori dell'identità digitale accreditati sono tenuti ad effettuare le verifiche di cui ai precedenti periodi.»

Note all'art. 4:

— Per il decreto del Presidente della Repubblica 15 gennaio 2018, n. 15, v. nelle note alle premesse.

Note all'art. 7:

— Per il decreto legislativo 18 maggio 2018, n. 51, v. nelle note alle premesse.

Note all'art. 11:

— Per il testo degli articoli 35, comma 4 e 55, primo comma, terzo periodo, del regio decreto 18 giugno 1931, n. 773, v. nelle note alle premesse.

Note all'art. 13:

— Per il testo degli articoli 35 e 55, del regio decreto 18 giugno 1931, n. 773, v. nelle note alle premesse.

Note all'art. 17:

— Per il testo degli articoli 35 e 55, del regio decreto 18 giugno 1931, n. 773, v. nelle note alle premesse.

— Per il Regolamento (CE) del 23 luglio 910/2014, v. nelle note alle premesse.

Note all'art. 19:

— Si riporta il testo dell'articolo 13, comma 2, della legge 3 agosto 2007, n. 124 (Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto):

«Art. 13 *(Collaborazione richiesta a pubbliche amministrazioni e a soggetti erogatori di servizi di pubblica utilità). — Omissis*.

2. Con apposito regolamento, adottato previa consultazione con le amministrazioni e i soggetti interessati, sono emanate le disposizioni necessarie ad assicurare l'accesso del DIS, dell'AISE e dell'AISI agli archivi informatici delle pubbliche amministrazioni e dei soggetti che erogano, in regime di autorizzazione, concessione o convenzione, servizi di pubblica utilità, prevedendo in ogni caso le modalità tecniche che consentano la verifica, anche successiva, dell'accesso a dati personali.

Omissis.»

Note all'art. 20:

Si riporta il testo dell'articolo 10, comma 3, del decreto del Ministro dell'interno 6 febbraio 2020:

«Art. 10 *(Ufficio VI – Sicurezza dati della Polizia di Stato). — Omissis*.

3. All'Ufficio sicurezza dati è preposto un Dirigente Superiore della carriera dei funzionari della Polizia di Stato che espletano funzioni di polizia, anche con compiti di data protection officer e di raccordo con il Garante per la protezione dei dati personali ai fini dello svolgimento delle relative attività di controllo.

Omissis.»

Note all'art. 24:

— Si riporta il testo degli articoli 8, 10, e 11, del citato regio decreto 18 giugno 1931, n. 773:

«Art. 8

Le autorizzazioni di polizia sono personali: non possono in alcun modo essere trasmesse nè dar luogo a rapporti di rappresentanza, salvi i casi espressamente preveduti dalla legge.

Nei casi in cui è consentita la rappresentanza nell'esercizio di una autorizzazione di polizia, il rappresentante deve possedere i requisiti necessari per conseguire l'autorizzazione e ottenere l'approvazione dell'autorità di pubblica sicurezza che ha conceduta l'autorizzazione.»

«Art. 10

Le autorizzazioni di polizia possono essere revocate o sospese in qualsiasi momento, nel caso di abuso della persona autorizzata.»

«Art. 11

Salve le condizioni particolari stabilite dalla legge nei singoli casi, le autorizzazioni di polizia debbono essere negate:

1° a chi ha riportato una condanna a pena restrittiva della libertà personale superiore a tre anni per delitto non colposo e non ha ottenuto la riabilitazione;

2° a chi è sottoposto all'ammonizione o a misura di sicurezza personale o è stato dichiarato delinquente abituale, professionale o per tendenza.

Le autorizzazioni di polizia possono essere negate a chi ha riportato condanna per delitti contro la personalità dello stato o contro l'ordine pubblico, ovvero per delitti contro le persone commessi con violenza, o per furto, rapina, estorsione, sequestro di persona a scopo di rapina o di estorsione, o per violenza o resistenza all'autorità, e a chi non può provare la sua buona condotta.

Le autorizzazioni devono essere revocate quando nella persona autorizzata vengono a mancare, in tutto o in parte, le condizioni alle quali sono subordinate, e possono essere revocate quando sopraggiungono o vengono a risultare circostanze che avrebbero imposto o consentito il diniego della autorizzazione.».

— Per il testo degli articoli 35 e 55 del regio decreto 18 giugno 1931, n. 773 v. nelle note alle premesse.

Note all'art. 26:

— Per il testo dell'articolo 10 del regio decreto 18 giugno 1931, n. 773, v. nelle note all'art. 24.

Note all'art. 27:

— Per il testo degli articoli 35 e 55, del regio decreto 18 giugno 1931, n. 773, v. nelle note alle premesse.

Note all'art. 29:

— Si riporta il testo dell'articolo 101, del decreto legislativo 22 gennaio 2004, n. 42 (Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137):

«Art. 101 *(Istituti e luoghi della cultura).* — 1. Ai fini del presente codice sono istituti e luoghi della cultura i musei, le biblioteche e gli archivi, le aree e i parchi archeologici, i complessi monumentali.

2. Si intende per:

a) «museo», una struttura permanente che acquisisce, cataloga, conserva, ordina ed espone beni culturali per finalità di educazione e di studio;

b) «biblioteca», una struttura permanente che raccoglie, cataloga e conserva un insieme organizzato di libri, materiali e informazioni, comunque editi o pubblicati su qualunque supporto, e ne assicura la consultazione al fine di promuovere la lettura e lo studio; (207)

c) «archivio», una struttura permanente che raccoglie, inventaria e conserva documenti originali di interesse storico e ne assicura la consultazione per finalità di studio e di ricerca;

d) «area archeologica», un sito caratterizzato dalla presenza di resti di natura fossile o di manufatti o strutture preistorici o di età antica;

e) «parco archeologico», un ambito territoriale caratterizzato da importanti evidenze archeologiche e dalla compresenza di valori storici, paesaggistici o ambientali, attrezzato come museo all'aperto;

f) «complesso monumentale», un insieme formato da una pluralità di fabbricati edificati anche in epoche diverse, che con il tempo hanno acquisito, come insieme, una autonoma rilevanza artistica, storica o etnoantropologica.

3. Gli istituti ed i luoghi di cui al comma 1 che appartengono a soggetti pubblici sono destinati alla pubblica fruizione ed espletano un servizio pubblico.

4. Le strutture espositive e di consultazione nonché i luoghi di cui al comma 1 che appartengono a soggetti privati e sono aperti al pubblico espletano un servizio privato di utilità sociale.»

— Si riporta il testo dell'articolo 32, primo comma, della citata legge 18 aprile 1975, n. 110:

«Art. 32 *(Vigilanza sulle armi e munizioni raccolte nei musei).*— Salva la normativa concernente le armi in dotazione alle Forze armate o ai Corpi armati dello Stato e fermo restando quanto stabilito nella legge 1 giugno 1939, n. 1089, sulle cose di interesse storico o artistico, i direttori dei musei di Stato, di altri enti pubblici o appartenenti ad enti morali, cui è affidata la custodia e la conservazione di raccolte di armi da guerra o tipo guerra o di parte di esse, di munizioni da guerra, di collezioni di armi comuni da sparo, di collezioni di armi artistiche, rare o antiche devono, entro tre mesi dall'entrata in vigore della presente legge, redigere l'inventario dei materiali custoditi su apposito registro ai sensi dell'art. 16, primo comma, del regio decreto 6 maggio 1940, n. 635.

Omissis.»

Note all'art. 31:

— Per il testo degli articoli 35 e 55, del regio decreto 18 giugno 1931, n. 773, v. nelle note alle premesse.

Note all'art. 32:

— Si riporta il testo dell'articolo 26 del citato decreto legislativo 18 maggio 2018, n. 51:

«Art. 26 *(Notifica al Garante di una violazione di dati personali).* — 1. Salvo quanto previsto dall'articolo 37, comma 6, in caso di violazione di dati personali, il titolare del trattamento notifica la violazione al Garante con le modalità di cui all'articolo 33 del regolamento UE.

2. Se la violazione dei dati personali riguarda dati personali che sono stati trasmessi dal o al titolare del trattamento di un altro Stato membro, le informazioni previste dal citato articolo 33 del regolamento UE sono comunicate, senza ingiustificato ritardo, al titolare del trattamento di tale Stato membro.»

Note all'art. 33:

— Per il regolamento delegato (UE) del 16 gennaio 2019, n. 686, v. nelle note alle premesse.

Note all'art. 35:

— Si riporta il testo dell'articolo 7, della legge 11 novembre 2011, n. 180 (Norme per la tutela della libertà d'impresa. Statuto delle imprese):

«Art. 7 *(Riduzione e trasparenza degli adempimenti amministrativi a carico di cittadini e imprese)*

1. Allo scopo di ridurre gli oneri informativi gravanti su cittadini e imprese, i regolamenti ministeriali o interministeriali, nonché i provvedimenti amministrativi a carattere generale adottati dalle amministrazioni dello Stato al fine di regolare l'esercizio di poteri autorizzatori, concessori o certificatori, nonché l'accesso ai servizi pubblici ovvero la concessione di benefici devono recare in allegato l'elenco di tutti gli oneri informativi gravanti sui cittadini e sulle imprese introdotti o eliminati con gli atti medesimi. Per onere informativo si intende qualunque adempimento che comporti la raccolta, l'elaborazione, la trasmissione, la conservazione e la produzione di informazioni e documenti alla pubblica amministrazione.

2. Gli atti di cui al comma 1, anche se pubblicati nella *Gazzetta Ufficiale*, sono pubblicati nei siti istituzionali di ciascuna amministrazione secondo i criteri e le modalità definiti con apposito regolamento da emanare con decreto del Presidente del Consiglio dei Ministri, su proposta del Ministro per la pubblica amministrazione e l'innovazione, entro novanta giorni dalla data di entrata in vigore della presente legge.

3. Il Dipartimento della funzione pubblica predispone, entro il 31 marzo di ciascun anno, una relazione annuale sullo stato di attuazione delle disposizioni di cui ai commi 1 e 2, valuta il loro impatto in termini di semplificazione e riduzione degli adempimenti amministrativi per i cittadini e le imprese, anche utilizzando strumenti di consultazione delle categorie e dei soggetti interessati, e la trasmette al Parlamento.

4. Con il regolamento di cui al comma 2, ai fini della valutazione degli eventuali profili di responsabilità dei dirigenti preposti agli uffici interessati, sono individuate le modalità di presentazione dei reclami da parte dei cittadini e delle imprese per la mancata applicazione delle disposizioni del presente articolo.»

23G00124