

LEGGI ED ALTRI ATTI NORMATIVI

LEGGE 23 settembre 2025, n. 132.

Disposizioni e deleghe al Governo in materia di intelligenza artificiale.

La Camera dei deputati ed il Senato della Repubblica hanno approvato;

IL PRESIDENTE DELLA REPUBBLICA

PROMULGA

la seguente legge:

Capo I

PRINCIPI E FINALITÀ

Art. 1.

Finalità e ambito di applicazione

1. La presente legge reca principi in materia di ricerca, sperimentazione, sviluppo, adozione e applicazione di sistemi e di modelli di intelligenza artificiale. Promuove un utilizzo corretto, trasparente e responsabile, in una dimensione antropocentrica, dell'intelligenza artificiale, volto a coglierne le opportunità. Garantisce la vigilanza sui rischi economici e sociali e sull'impatto sui diritti fondamentali dell'intelligenza artificiale.

2. Le disposizioni della presente legge si interpretano e si applicano conformemente al regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024.

Art. 2.

Definizioni

1. Ai fini della presente legge, si intendono per:

a) sistema di intelligenza artificiale: il sistema definito dall'articolo 3, punto 1), del regolamento (UE) 2024/1689;

b) dato: qualsiasi rappresentazione digitale di atti, fatti o informazioni e qualsiasi raccolta di tali atti, fatti o informazioni, anche sotto forma di registrazione sonora, visiva o audiovisiva;

c) modelli di intelligenza artificiale: i modelli definiti dall'articolo 3, punto 63), del regolamento (UE) 2024/1689.

2. Per quanto non espressamente previsto, si rimanda alle definizioni di cui al regolamento (UE) 2024/1689.

Art. 3.

Principi generali

1. La ricerca, la sperimentazione, lo sviluppo, l'adozione, l'applicazione e l'utilizzo di sistemi e di modelli di intelligenza artificiale per finalità generali avvengono nel rispetto dei diritti fondamentali e delle libertà previste dalla Costituzione, del diritto dell'Unione europea e dei

principi di trasparenza, proporzionalità, sicurezza, protezione dei dati personali, riservatezza, accuratezza, non discriminazione, parità dei sessi e sostenibilità.

2. Lo sviluppo di sistemi e di modelli di intelligenza artificiale per finalità generali avviene su dati e tramite processi di cui devono essere garantite e vigilate la correttezza, l'attendibilità, la sicurezza, la qualità, l'appropriatezza e la trasparenza, secondo il principio di proporzionalità in relazione ai settori nei quali sono utilizzati.

3. I sistemi e i modelli di intelligenza artificiale per finalità generali devono essere sviluppati e applicati nel rispetto dell'autonomia e del potere decisionale dell'uomo, della prevenzione del danno, della conoscibilità, della trasparenza, della spiegabilità e dei principi di cui al comma 1, assicurando la sorveglianza e l'intervento umano.

4. L'utilizzo di sistemi di intelligenza artificiale non deve pregiudicare lo svolgimento con metodo democratico della vita istituzionale e politica e l'esercizio delle competenze e funzioni delle istituzioni territoriali sulla base dei principi di autonomia e sussidiarietà e non deve altresì pregiudicare la libertà del dibattito democratico da interferenze illecite, da chiunque provocate, tutelando gli interessi della sovranità dello Stato nonché i diritti fondamentali di ogni cittadino riconosciuti dagli ordinamenti nazionale ed europeo.

5. La presente legge non produce nuovi obblighi rispetto a quelli previsti dal regolamento (UE) 2024/1689 per i sistemi di intelligenza artificiale e per i modelli di intelligenza artificiale per finalità generali.

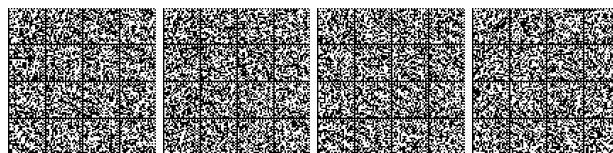
6. Al fine di garantire il rispetto dei diritti e dei principi di cui al presente articolo deve essere assicurata, quale condizione essenziale, la cybersicurezza lungo tutto il ciclo di vita dei sistemi e dei modelli di intelligenza artificiale per finalità generali, secondo un approccio proporzionale e basato sul rischio, nonché l'adozione di specifici controlli di sicurezza, anche al fine di assicurarne la resilienza contro tentativi di alterarne l'utilizzo, il comportamento previsto, le prestazioni o le impostazioni di sicurezza.

7. La presente legge garantisce alle persone con disabilità il pieno accesso ai sistemi di intelligenza artificiale e alle relative funzionalità o estensioni, su base di uguaglianza e senza alcuna forma di discriminazione e di pregiudizio, in conformità alle disposizioni della Convenzione delle Nazioni Unite sui diritti delle persone con disabilità, fatta a New York il 13 dicembre 2006, ratificata e resa esecutiva in Italia ai sensi della legge 3 marzo 2009, n. 18.

Art. 4.

Principi in materia di informazione e di riservatezza dei dati personali

1. L'utilizzo di sistemi di intelligenza artificiale nell'informazione avviene senza recare pregiudizio alla libertà e al pluralismo dei mezzi di comunicazione, alla libertà di espressione e all'obiettività, completezza, imparzialità e lealtà dell'informazione.



2. L'utilizzo di sistemi di intelligenza artificiale garantisce il trattamento lecito, corretto e trasparente dei dati personali e la compatibilità con le finalità per le quali sono stati raccolti, in conformità al diritto dell'Unione europea in materia di dati personali e di tutela della riservatezza.

3. Le informazioni e le comunicazioni relative al trattamento dei dati connesse all'utilizzo di sistemi di intelligenza artificiale sono rese con linguaggio chiaro e semplice, in modo da garantire all'utente la conoscibilità dei relativi rischi e il diritto di opporsi ai trattamenti autorizzati dei propri dati personali.

4. L'accesso alle tecnologie di intelligenza artificiale da parte dei minori di anni quattordici nonché il conseguente trattamento dei dati personali richiedono il consenso di chi esercita la responsabilità genitoriale, nel rispetto di 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. Il minore di anni diciotto, che abbia compiuto quattordici anni, può esprimere il proprio consenso per il trattamento dei dati personali connessi all'utilizzo di sistemi di intelligenza artificiale, purché le informazioni e le comunicazioni di cui al comma 3 siano facilmente accessibili e comprensibili.

Art. 5.

Principi in materia di sviluppo economico

1. Lo Stato e le altre autorità pubbliche:

a) promuovono lo sviluppo e l'utilizzo dell'intelligenza artificiale come strumento per migliorare l'interazione uomo-macchina, anche mediante l'applicazione della robotica, nei settori produttivi, la produttività in tutte le catene del valore e le funzioni organizzative, nonché quale strumento utile all'avvio di nuove attività economiche e di supporto al tessuto nazionale produttivo, costituito principalmente di microimprese e di piccole e medie imprese, al fine di accrescere la competitività del sistema economico nazionale e la sovranità tecnologica della Nazione nel quadro della strategia europea;

b) favoriscono la creazione di un mercato dell'intelligenza artificiale innovativo, equo, aperto e concorrenziale e di ecosistemi innovativi;

c) facilitano la disponibilità e l'accesso a dati di alta qualità per le imprese che sviluppino o utilizzino sistemi di intelligenza artificiale e per la comunità scientifica e dell'innovazione;

d) indirizzano le piattaforme di *e-procurement* delle amministrazioni pubbliche di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, in modo che, nella scelta dei fornitori di sistemi e di modelli di intelligenza artificiale, possano essere privilegiate quelle soluzioni che garantiscono la localizzazione e l'elaborazione dei dati strategici presso *data center* posti nel territorio nazionale, le cui procedure di *disaster recovery* e *business continuity* siano implementate in *data center* posti nel territorio nazionale, nonché modelli in grado di assicurare elevati standard in termini di sicurezza e tra-

sparenza nelle modalità di addestramento e di sviluppo di applicazioni basate sull'intelligenza artificiale generativa, nel rispetto della normativa sulla concorrenza e dei principi di non discriminazione e proporzionalità;

e) favoriscono la ricerca collaborativa tra imprese, organismi di ricerca e centri di trasferimento tecnologico in materia di intelligenza artificiale al fine di incoraggiare la valorizzazione economica e commerciale dei risultati della ricerca.

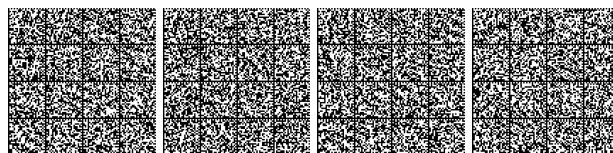
Art. 6.

Disposizioni in materia di sicurezza e difesa nazionale

1. Le attività di cui all'articolo 3, comma 1, svolte per scopi di sicurezza nazionale con le finalità e le modalità di cui alla legge 3 agosto 2007, n. 124, dagli organismi di cui agli articoli 4, 6 e 7 della medesima legge, quelle di cybersicurezza e di resilienza di cui all'articolo 1, comma 1, lettere a) e b), del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, svolte dall'Agenzia per la cybersicurezza nazionale a tutela della sicurezza nazionale nello spazio cibernetico, quelle svolte per scopi di difesa nazionale dalle Forze armate nonché quelle svolte dalle Forze di polizia dirette a prevenire e contrastare, ai fini della sicurezza nazionale, i reati di cui all'articolo 9, comma 1, lettere b) e b-ter), della legge 16 marzo 2006, n. 146, sono escluse dall'ambito applicativo della presente legge. Le medesime attività sono comunque effettuate nel rispetto dei diritti fondamentali e delle libertà previste dalla Costituzione e di quanto disposto dall'articolo 3, comma 4, della presente legge.

2. Lo sviluppo di sistemi e di modelli di intelligenza artificiale avviene nel rispetto delle condizioni e delle finalità di cui all'articolo 3, comma 2. Ai trattamenti di dati personali mediante l'utilizzo di sistemi di intelligenza artificiale effettuati dagli organismi di cui agli articoli 4, 6 e 7 della legge n. 124 del 2007 si applica quanto previsto dall'articolo 58, commi 1 e 3, del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196. Ai trattamenti di dati personali mediante l'utilizzo di sistemi di intelligenza artificiale effettuati dall'Agenzia per la cybersicurezza nazionale si applicano le disposizioni di cui all'articolo 13 del citato decreto-legge n. 82 del 2021.

3. Con regolamento adottato ai sensi dell'articolo 43 della legge n. 124 del 2007, sono definite le modalità di applicazione dei principi e delle disposizioni di cui al presente articolo alle attività di cui all'articolo 3, comma 1, della presente legge effettuate dagli organismi di cui agli articoli 4, 6 e 7 della legge n. 124 del 2007, nonché alle medesime attività attinenti a sistemi di intelligenza artificiale, funzionali all'attività degli organismi stessi e alle medesime attività svolte da altri soggetti pubblici e da soggetti privati esclusivamente per scopi di sicurezza nazionale. Analogamente, per l'Agenzia per la cybersicurezza nazionale si procede con regolamento adottato secondo le modalità di cui all'articolo 11, comma 4, del citato decreto-legge n. 82 del 2021.



Capo II

DISPOSIZIONI DI SETTORE

Art. 7.

*Uso dell'intelligenza artificiale
in ambito sanitario e di disabilità*

1. L'utilizzo di sistemi di intelligenza artificiale contribuisce al miglioramento del sistema sanitario, alla prevenzione, alla diagnosi e alla cura delle malattie, nel rispetto dei diritti, delle libertà e degli interessi della persona, anche in materia di protezione dei dati personali.

2. L'introduzione di sistemi di intelligenza artificiale nel sistema sanitario non può selezionare e condizionare l'accesso alle prestazioni sanitarie secondo criteri discriminatori.

3. L'interessato ha diritto di essere informato sull'impiego di tecnologie di intelligenza artificiale.

4. La presente legge promuove lo sviluppo, lo studio e la diffusione di sistemi di intelligenza artificiale che migliorano le condizioni di vita delle persone con disabilità, agevolano l'accessibilità, la mobilità indipendente e l'autonomia, la sicurezza e i processi di inclusione sociale delle medesime persone anche ai fini dell'elaborazione del progetto di vita di cui all'articolo 2, comma 1, lettera n), del decreto legislativo 3 maggio 2024, n. 62.

5. I sistemi di intelligenza artificiale in ambito sanitario costituiscono un supporto nei processi di prevenzione, diagnosi, cura e scelta terapeutica, lasciando impregiudicata la decisione, che è sempre rimessa agli esercenti la professione medica.

6. I sistemi di intelligenza artificiale utilizzati in ambito sanitario e i relativi dati impiegati devono essere affidabili, periodicamente verificati e aggiornati al fine di minimizzare il rischio di errori e migliorare la sicurezza dei pazienti.

Art. 8.

*Ricerca e sperimentazione scientifica nella realizzazione
di sistemi di intelligenza artificiale in ambito sanitario*

1. I trattamenti di dati, anche personali, eseguiti da soggetti pubblici e privati senza scopo di lucro, dagli Istituti di ricovero e cura a carattere scientifico (IRCCS), di cui al decreto legislativo 16 ottobre 2003, n. 288, nonché da soggetti privati operanti nel settore sanitario nell'ambito di progetti di ricerca a cui partecipano soggetti pubblici e privati senza scopo di lucro o IRCCS, per la ricerca e la sperimentazione scientifica nella realizzazione di sistemi di intelligenza artificiale per finalità di prevenzione, diagnosi e cura di malattie, sviluppo di farmaci, terapie e tecnologie riabilitative, realizzazione di apparati medicali, incluse protesi e interfacce fra il corpo e strumenti di sostegno alle condizioni del paziente, salute pubblica, incolumità della persona, salute e sicurezza sanitaria nonché studio della fisiologia, della biomeccanica e della biologia umana anche in ambito non sanitario, in quanto necessari ai fini della realizzazione e dell'utilizzazione di banche di dati e modelli di base, sono dichiarati di rilevante interesse pubblico in attuazione degli articoli 32

e 33 della Costituzione e nel rispetto di quanto previsto dall'articolo 9, paragrafo 2, lettera g), del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016.

2. Ai medesimi fini, fermo restando l'obbligo di informativa in favore dell'interessato, che può essere assolto anche mediante un'informativa generale messa a disposizione nel sito *web* del titolare del trattamento e senza ulteriore consenso dell'interessato ove inizialmente previsto dalla legge, è sempre autorizzato l'uso secondario di dati personali privi degli elementi identificativi diretti, anche appartenenti alle categorie indicate all'articolo 9 del regolamento (UE) 2016/679, da parte dei soggetti di cui al comma 1, salvi i casi nei quali la conoscenza dell'identità degli interessati sia inevitabile o necessaria al fine della tutela della loro salute.

3. Negli ambiti di cui al comma 1 o per le finalità di cui all'articolo 2-sexies, comma 2, lettera v), del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196, è sempre consentito, previa informativa all'interessato ai sensi dell'articolo 13 del regolamento (UE) 2016/679, il trattamento per finalità di anonimizzazione, pseudonimizzazione o sintetizzazione dei dati personali, anche appartenenti alle categorie particolari di cui all'articolo 9, paragrafo 1, del medesimo regolamento (UE) 2016/679. È consentito altresì il predetto trattamento finalizzato allo studio e alla ricerca sui gesti atletici, sui movimenti e sulle prestazioni nell'attività sportiva in tutte le sue forme, nel rispetto dei principi generali di cui alla presente legge e dei diritti di sfruttamento economico dei dati relativi alle attività agonistiche che spettano a chi le organizza.

4. L'Agenzia nazionale per i servizi sanitari regionali (AGENAS), previo parere del Garante per la protezione dei dati personali, tenendo conto di *standard* internazionali e dello stato dell'arte e della tecnica, può stabilire e aggiornare linee guida per le procedure di anonimizzazione di dati personali, di cui al comma 3, e per la creazione di dati sintetici, anche per categorie di dati e finalità di trattamento.

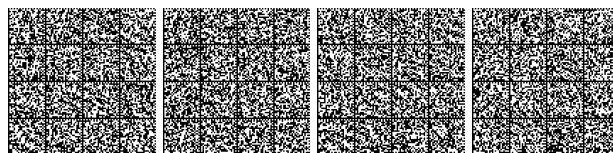
5. I trattamenti di dati di cui ai commi 1 e 2 devono essere comunicati al Garante per la protezione dei dati personali con l'indicazione di tutte le informazioni previste dagli articoli 24, 25, 32 e 35 del regolamento (UE) 2016/679, nonché con l'indicazione espressa, ove presenti, dei soggetti individuati ai sensi dell'articolo 28 del medesimo regolamento (UE) 2016/679, e possono essere avviati decorsi trenta giorni dalla predetta comunicazione se non sono stati oggetto di provvedimento di blocco disposto dal Garante per la protezione dei dati personali.

6. Restano fermi i poteri ispettivi, interdittivi e sanzionatori del Garante per la protezione dei dati personali.

Art. 9.

Disposizioni in materia di trattamento di dati personali

1. Il trattamento dei dati personali anche particolari come definiti dall'articolo 9 del regolamento (UE) 2016/679, con il massimo delle modalità semplificate consentite dal predetto regolamento per finalità di ricerca e sperimentazione anche tramite sistemi di intelligen-



za artificiale e *machine learning*, inclusi la costituzione e l'utilizzo di spazi speciali di sperimentazione a fini di ricerca, anche mediante l'uso secondario dei dati personali, è disciplinato con decreto del Ministro della salute da emanare entro centoventi giorni dalla data di entrata in vigore della presente legge, sentiti il Garante per la protezione dei dati personali, gli enti di ricerca, i presidi sanitari nonché le autorità e gli operatori del settore.

Art. 10.

Disposizioni in materia di fascicolo sanitario elettronico, sistemi di sorveglianza nel settore sanitario e governo della sanità digitale

1. Al decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, dopo l'articolo 12 è inserito il seguente:

«Art. 12-bis (*Intelligenza artificiale nel settore sanitario*). — 1. Al fine di garantire strumenti e tecnologie avanzate nel settore sanitario, con uno o più decreti del Ministro della salute, di concerto con l'Autorità politica delegata in materia di innovazione tecnologica e transizione digitale e con l'Autorità delegata per la sicurezza della Repubblica e per la cybersicurezza e sentita la Conferenza permanente per i rapporti tra lo Stato, le regioni e le province autonome di Trento e di Bolzano, sono disciplinate le soluzioni di intelligenza artificiale aventi funzione di supporto alle finalità di cui all'articolo 12, comma 2. Con i decreti di cui al primo periodo sono individuati i soggetti che, nell'esercizio delle proprie funzioni, accedono alle soluzioni di intelligenza artificiale secondo le modalità ivi definite.

2. Per il supporto alle finalità di cura, e in particolare per l'assistenza territoriale, è istituita una piattaforma di intelligenza artificiale. La progettazione, la realizzazione, la messa in servizio e la titolarità della piattaforma di cui al primo periodo sono attribuite all'AGENAS in qualità di Agenzia nazionale per la sanità digitale. La piattaforma di cui al primo periodo eroga servizi di supporto:

a) ai professionisti sanitari per la presa in carico della popolazione assistita con suggerimenti non vincolanti;

b) ai medici nella pratica clinica quotidiana con suggerimenti non vincolanti;

c) agli utenti per l'accesso ai servizi sanitari delle Case della comunità.

3. Previa intesa in sede di Conferenza permanente per i rapporti tra lo Stato, le regioni e le province autonome di Trento e di Bolzano, l'AGENAS, con proprio provvedimento, esplicita i servizi di supporto di cui al comma 2.

4. La piattaforma di cui al comma 2 è alimentata con i dati strettamente necessari per l'erogazione dei servizi di cui al medesimo comma 2, trasmessi dai relativi titolari del trattamento. L'AGENAS è titolare del trattamento dei dati raccolti e generati all'interno della piattaforma.

5. Previo parere del Ministero della salute, del Garante per la protezione dei dati personali e dell'Agenzia per la cybersicurezza nazionale, l'AGENAS, con proprio

provvedimento, valutato l'impatto del trattamento, specifica i tipi di dati trattati e le operazioni eseguite all'interno della piattaforma, nonché le misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio e per tutelare i diritti fondamentali e gli interessi dell'interessato, in coerenza con le disposizioni del regolamento (UE) 2016/679».

2. Dall'attuazione del presente articolo non devono derivare nuovi o maggiori oneri a carico della finanza pubblica. L'AGENAS provvede alle attività di cui al presente articolo con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente.

Art. 11.

Disposizioni sull'uso dell'intelligenza artificiale in materia di lavoro

1. L'intelligenza artificiale è impiegata per migliorare le condizioni di lavoro, tutelare l'integrità psicofisica dei lavoratori, accrescere la qualità delle prestazioni lavorative e la produttività delle persone in conformità al diritto dell'Unione europea.

2. L'utilizzo dell'intelligenza artificiale in ambito lavorativo deve essere sicuro, affidabile, trasparente e non può svolgersi in contrasto con la dignità umana né violare la riservatezza dei dati personali. Il datore di lavoro o il committente è tenuto a informare il lavoratore dell'utilizzo dell'intelligenza artificiale nei casi e con le modalità di cui all'articolo 1-bis del decreto legislativo 26 maggio 1997, n. 152.

3. L'intelligenza artificiale nell'organizzazione e nella gestione del rapporto di lavoro garantisce l'osservanza dei diritti inviolabili del lavoratore senza discriminazioni in funzione del sesso, dell'età, delle origini etniche, del credo religioso, dell'orientamento sessuale, delle opinioni politiche e delle condizioni personali, sociali ed economiche, in conformità al diritto dell'Unione europea.

Art. 12.

Osservatorio sull'adozione di sistemi di intelligenza artificiale nel mondo del lavoro

1. Al fine di massimizzare i benefici e contenere i rischi derivanti dall'impiego di sistemi di intelligenza artificiale in ambito lavorativo, è istituito presso il Ministero del lavoro e delle politiche sociali l'Osservatorio sull'adozione di sistemi di intelligenza artificiale nel mondo del lavoro, con il compito di definire una strategia sull'utilizzo dell'intelligenza artificiale in ambito lavorativo, monitorare l'impatto sul mercato del lavoro e identificare i settori lavorativi maggiormente interessati dall'avvento dell'intelligenza artificiale. L'Osservatorio promuove la formazione dei lavoratori e dei datori di lavoro in materia di intelligenza artificiale.

2. L'Osservatorio è presieduto dal Ministro del lavoro e delle politiche sociali o da un suo rappresentante. Con decreto del Ministro del lavoro e delle politiche sociali, da adottare entro novanta giorni dalla data di entrata in vigore della presente legge, sono stabiliti i componenti, le



modalità di funzionamento, nonché gli ulteriori compiti e funzioni dell'Osservatorio medesimo. Ai componenti dell'Osservatorio non spettano compensi, gettoni di presenza, rimborsi di spese o altri emolumenti comunque denominati.

3. All'istituzione e al funzionamento dell'Osservatorio si provvede nell'ambito delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente.

Art. 13.

Disposizioni in materia di professioni intellettuali

1. L'utilizzo di sistemi di intelligenza artificiale nelle professioni intellettuali è finalizzato al solo esercizio delle attività strumentali e di supporto all'attività professionale e con prevalenza del lavoro intellettuale oggetto della prestazione d'opera.

2. Per assicurare il rapporto fiduciario tra professionista e cliente, le informazioni relative ai sistemi di intelligenza artificiale utilizzati dal professionista sono comunicate al soggetto destinatario della prestazione intellettuale con linguaggio chiaro, semplice ed esaustivo.

Art. 14.

Uso dell'intelligenza artificiale nella pubblica amministrazione

1. Le pubbliche amministrazioni utilizzano l'intelligenza artificiale allo scopo di incrementare l'efficienza della propria attività, di ridurre i tempi di definizione dei procedimenti e di aumentare la qualità e la quantità dei servizi erogati ai cittadini e alle imprese, assicurando agli interessati la conoscibilità del suo funzionamento e la tracciabilità del suo utilizzo.

2. L'utilizzo dell'intelligenza artificiale avviene in funzione strumentale e di supporto all'attività provvedimentale, nel rispetto dell'autonomia e del potere decisionale della persona che resta l'unica responsabile dei provvedimenti e dei procedimenti in cui sia stata utilizzata l'intelligenza artificiale.

3. Le pubbliche amministrazioni adottano misure tecniche, organizzative e formative finalizzate a garantire un utilizzo responsabile dell'intelligenza artificiale e a sviluppare le capacità trasversali degli utilizzatori.

4. Le pubbliche amministrazioni provvedono agli adempimenti previsti dal presente articolo con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente.

Art. 15.

Impiego dei sistemi di intelligenza artificiale nell'attività giudiziaria

1. Nei casi di impiego dei sistemi di intelligenza artificiale nell'attività giudiziaria è sempre riservata al magistrato ogni decisione sull'interpretazione e sull'applicazione della legge, sulla valutazione dei fatti e delle prove e sull'adozione dei provvedimenti.

2. Il Ministero della giustizia disciplina gli impieghi dei sistemi di intelligenza artificiale per l'organizzazio-

ne dei servizi relativi alla giustizia, per la semplificazione del lavoro giudiziario e per le attività amministrative accessorie.

3. Fino alla compiuta attuazione del regolamento (UE) 2024/1689, la sperimentazione e l'impiego dei sistemi di intelligenza artificiale negli uffici giudiziari ordinari sono autorizzati dal Ministero della giustizia, sentite le Autorità nazionali di cui all'articolo 20.

4. Il Ministro della giustizia, nell'elaborazione delle linee programmatiche sulla formazione dei magistrati di cui all'articolo 12, comma 1, lettera a), del decreto legislativo 30 gennaio 2006, n. 26, promuove attività didattiche sul tema dell'intelligenza artificiale e sugli impieghi dei sistemi di intelligenza artificiale nell'attività giudiziaria, finalizzate alla formazione digitale di base e avanzata, all'acquisizione e alla condivisione di competenze digitali, nonché alla sensibilizzazione sui benefici e rischi, anche nel quadro regolatorio di cui ai commi 2 e 3 del presente articolo. Per le medesime finalità di cui al primo periodo, il Ministro cura altresì la formazione del personale amministrativo.

Art. 16.

Delega al Governo in materia di dati, algoritmi e metodi matematici per l'addestramento di sistemi di intelligenza artificiale

1. Il Governo è delegato ad adottare, entro dodici mesi dalla data di entrata in vigore della presente legge, uno o più decreti legislativi per definire una disciplina organica relativa all'utilizzo di dati, algoritmi e metodi matematici per l'addestramento di sistemi di intelligenza artificiale senza obblighi ulteriori, negli ambiti soggetti al regolamento (UE) 2024/1689, rispetto a quanto già ivi stabilito.

2. Gli schemi dei decreti legislativi di cui al comma 1 sono adottati su proposta del Presidente del Consiglio dei ministri e del Ministro della giustizia e sono successivamente trasmessi alle Camere per l'espressione del parere delle Commissioni parlamentari competenti. Decorsi sessanta giorni dalla data della trasmissione, i decreti possono essere emanati anche in mancanza dei pareri. Qualora detto termine venga a scadere nei trenta giorni antecedenti alla scadenza del termine previsto per l'esercizio della delega o successivamente, quest'ultimo è prorogato di sessanta giorni.

3. Nell'esercizio della delega di cui al comma 1, il Governo si attiene ai seguenti principi e criteri direttivi:

a) individuare ipotesi per le quali appare necessario dettare il regime giuridico dell'utilizzo di dati, algoritmi e metodi matematici per l'addestramento di sistemi di intelligenza artificiale, nonché i diritti e gli obblighi gravanti sulla parte che intenda procedere al suddetto utilizzo;

b) prevedere strumenti di tutela, di carattere risarcitorio o inibitorio, e individuare un apparato sanzionatorio per il caso di violazione delle disposizioni introdotte ai sensi della lettera a);

c) attribuire alle sezioni specializzate in materia di impresa le controversie relative alla disciplina introdotta ai sensi delle lettere a) e b).



Art. 17.

Modifica al codice di procedura civile

1. All'articolo 9, secondo comma, del codice di procedura civile, dopo le parole: «esecuzione forzata» sono inserite le seguenti: «, per le cause che hanno ad oggetto il funzionamento di un sistema di intelligenza artificiale».

Art. 18.

Uso dell'intelligenza artificiale per il rafforzamento della cybersicurezza nazionale

1. All'articolo 7, comma 1, del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, dopo la lettera m-ter) è inserita la seguente:

«m-quater) promuove e sviluppa ogni iniziativa, anche attraverso la conclusione di accordi di collaborazione con i privati, comunque denominati, nonché di partenariato pubblico-privato, volta a valorizzare l'intelligenza artificiale come risorsa per il rafforzamento della cybersicurezza nazionale».

*Capo III*STRATEGIA NAZIONALE, AUTORITÀ NAZIONALI
E AZIONI DI PROMOZIONE

Art. 19.

Strategia nazionale per l'intelligenza artificiale e Comitato di coordinamento delle attività di indirizzo su enti, organismi e fondazioni che operano nel campo dell'innovazione digitale e dell'intelligenza artificiale

1. La strategia nazionale per l'intelligenza artificiale è predisposta e aggiornata dalla struttura della Presidenza del Consiglio dei ministri competente in materia di innovazione tecnologica e transizione digitale, d'intesa con le Autorità nazionali per l'intelligenza artificiale di cui all'articolo 20, sentiti il Ministro delle imprese e del made in Italy per i profili di politica industriale e di incentivazione, il Ministro dell'università e della ricerca per i profili relativi alla formazione superiore e alla ricerca e il Ministro della difesa per gli aspetti relativi ai sistemi di intelligenza artificiale impiegabili in chiave duale, ed è approvata con cadenza almeno biennale dal Comitato interministeriale per la transizione digitale (CITD) di cui all'articolo 8, comma 2, del decreto-legge 1° marzo 2021, n. 22, convertito, con modificazioni, dalla legge 22 aprile 2021, n. 55.

2. La strategia di cui al comma 1 favorisce la collaborazione tra le amministrazioni pubbliche e i soggetti privati relativamente allo sviluppo e all'adozione di sistemi di intelligenza artificiale, coordina l'attività della pubblica amministrazione in materia, promuove la ricerca e la diffusione della conoscenza in materia di intelligenza artificiale e indirizza le misure e gli incentivi finalizzati allo sviluppo imprenditoriale e industriale dell'intelligenza artificiale.

3. La strategia di cui al comma 1 tiene conto dei principi del diritto internazionale umanitario, al fine dello sviluppo e della promozione di sistemi di intelligenza artificiale che tutelino i diritti umani.

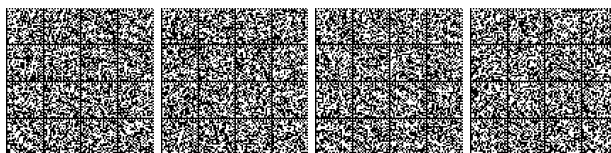
4. La struttura della Presidenza del Consiglio dei ministri competente in materia di innovazione tecnologica e transizione digitale provvede al coordinamento e al monitoraggio dell'attuazione della strategia di cui al comma 1, avvalendosi dell'Agenzia per l'Italia digitale, d'intesa, per gli aspetti di competenza, con l'Agenzia per la cybersicurezza nazionale e sentiti la Banca d'Italia, la Commissione nazionale per le società e la borsa (CONSOB) e l'Istituto per la vigilanza sulle assicurazioni (IVASS) in qualità di autorità di vigilanza del mercato. I risultati del monitoraggio sono trasmessi annualmente alle Camere.

5. All'articolo 8, comma 3, primo periodo, del decreto-legge 1° marzo 2021, n. 22, convertito, con modificazioni, dalla legge 22 aprile 2021, n. 55, dopo le parole: «delle imprese e del made in Italy» sono inserite le seguenti: «, dell'università e della ricerca» e sono aggiunte, in fine, le seguenti parole: «nonché dall'Autorità delegata per la sicurezza della Repubblica e per la cybersicurezza, ove nominata».

6. È istituito il Comitato di coordinamento delle attività di indirizzo su enti, organismi e fondazioni che operano nel campo dell'innovazione digitale e dell'intelligenza artificiale, presieduto dal Presidente del Consiglio dei ministri o dall'Autorità politica delegata e composto dal Ministro dell'economia e delle finanze, dal Ministro delle imprese e del made in Italy, dal Ministro dell'università e della ricerca, dal Ministro della salute, dal Ministro per la pubblica amministrazione, dall'Autorità delegata per la sicurezza della Repubblica e per la cybersicurezza e dall'Autorità politica delegata in materia di innovazione tecnologica e transizione digitale o da loro delegati. Alle sedute del Comitato possono essere invitati rappresentanti delle Autorità nazionali di cui all'articolo 20 nonché altri soggetti interessati agli argomenti trattati. Per la partecipazione al Comitato non spettano compensi, gettoni di presenza, rimborsi di spese o altri emolumenti comunque denominati.

7. Il Comitato di cui al comma 6, per assicurare la migliore realizzazione della strategia di cui al comma 1, svolge funzioni di coordinamento dell'azione di indirizzo e di promozione delle attività di ricerca, di sperimentazione, di sviluppo, di adozione e di applicazione di sistemi e modelli di intelligenza artificiale svolte da enti e organismi nazionali pubblici o privati soggetti a vigilanza o destinatari di finanziamento pubblico, ivi comprese le fondazioni pubbliche o private vigilate o finanziate dallo Stato, che operano nel campo dell'innovazione digitale e dell'intelligenza artificiale. Gli enti, gli organismi e le fondazioni di cui al periodo precedente sono individuati dal medesimo Comitato. Il Comitato svolge altresì funzioni di coordinamento delle attività di indirizzo sulle politiche di formazione nelle competenze digitali e dell'intelligenza artificiale svolte dai medesimi enti.

8. Dall'istituzione e dal funzionamento del Comitato di cui al comma 6 non devono derivare nuovi o maggiori oneri per la finanza pubblica. Le amministrazioni



competenti vi provvedono nell'ambito delle risorse umane, finanziarie e strumentali disponibili a legislazione vigente.

Art. 20.

Autorità nazionali per l'intelligenza artificiale

1. Al fine di garantire l'applicazione e l'attuazione della normativa nazionale e dell'Unione europea in materia di intelligenza artificiale, l'Agenzia per l'Italia digitale (AgID) e l'Agenzia per la cybersicurezza nazionale (ACN) sono designate quali Autorità nazionali per l'intelligenza artificiale, ferma restando l'attribuzione alla Banca d'Italia, alla CONSOB e all'IVASS del ruolo di autorità di vigilanza del mercato ai sensi e secondo quanto previsto dall'articolo 74, paragrafo 6, del regolamento (UE) 2024/1689. Conseguentemente, nel rispetto dei principi di cui alla presente legge e ferme restando le funzioni già rispettivamente attribuite:

a) l'AgID è responsabile di promuovere l'innovazione e lo sviluppo dell'intelligenza artificiale, fatto salvo quanto previsto dalla lettera b). L'AgID provvede altresì a definire le procedure e a esercitare le funzioni e i compiti in materia di notifica, valutazione, accreditamento e monitoraggio dei soggetti incaricati di verificare la conformità dei sistemi di intelligenza artificiale, secondo quanto previsto dalla normativa nazionale e dell'Unione europea;

b) l'ACN, anche ai fini di assicurare la tutela della cybersicurezza, come definita dall'articolo 1, comma 1, del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, è responsabile per la vigilanza, ivi incluse le attività ispettive e sanzionatorie, dei sistemi di intelligenza artificiale, secondo quanto previsto dalla normativa nazionale e dell'Unione europea. L'ACN è altresì responsabile per la promozione e lo sviluppo dell'intelligenza artificiale relativamente ai profili di cybersicurezza;

c) l'AgID e l'ACN, ciascuna per quanto di rispettiva competenza, assicurano l'istituzione e la gestione congiunta di spazi di sperimentazione finalizzati alla realizzazione di sistemi di intelligenza artificiale conformi alla normativa nazionale e dell'Unione europea, sentiti il Ministero della difesa per gli aspetti relativi ai sistemi di intelligenza artificiale impiegabili in chiave duale e il Ministero della giustizia per i modelli e i sistemi di intelligenza artificiale applicabili all'attività giudiziaria. Resta fermo quanto previsto dall'articolo 36, commi da 2-bis a 2-novies, del decreto-legge 30 aprile 2019, n. 34, convertito, con modificazioni, dalla legge 28 giugno 2019, n. 58, per quanto concerne la sperimentazione di sistemi di intelligenza artificiale destinati ad essere immessi sul mercato, messi in servizio o usati da istituti finanziari.

2. Ferma restando l'attribuzione alla Banca d'Italia, alla CONSOB e all'IVASS del ruolo di autorità di vigilanza del mercato ai sensi e secondo quanto previsto dall'articolo 74, paragrafo 6, del regolamento (UE) 2024/1689, l'AgID è designata quale autorità di notifica ai sensi dell'articolo 70 del medesimo regolamento e l'ACN è designata quale autorità di vigilanza del mercato

e punto di contatto unico con le istituzioni dell'Unione europea ai sensi del medesimo articolo 70.

3. Le Autorità nazionali per l'intelligenza artificiale di cui al comma 1 assicurano il coordinamento e la collaborazione con le altre pubbliche amministrazioni e le autorità indipendenti, nonché ogni opportuno raccordo tra loro per l'esercizio delle funzioni di cui al presente articolo. A quest'ultimo fine, presso la Presidenza del Consiglio dei ministri è istituito un Comitato di coordinamento, composto dai direttori generali delle due citate Agenzie e dal capo del Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei ministri medesima. Al suddetto Comitato partecipano, quando si trattano questioni di rispettiva competenza, rappresentanti di vertice della Banca d'Italia, della CONSOB e dell'IVASS. Ai componenti del Comitato non spettano compensi, gettoni di presenza, rimborsi di spese o altri emolumenti comunque denominati.

4. Restano fermi le competenze, i compiti e i poteri del Garante per la protezione dei dati personali e dell'Autorità per le garanzie nelle comunicazioni, quale Coordinatore dei Servizi Digitali ai sensi dell'articolo 15 del decreto-legge 15 settembre 2023, n. 123, convertito, con modificazioni, dalla legge 13 novembre 2023, n. 159.

5. All'articolo 8, comma 2, primo periodo, del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, dopo le parole: «Presidenza del Consiglio dei ministri» sono aggiunte le seguenti: «nonché dell'Agenzia per l'Italia digitale (AgID)».

Art. 21.

Applicazione sperimentale dell'intelligenza artificiale ai servizi forniti dal Ministero degli affari esteri e della cooperazione internazionale

1. È autorizzata la spesa di euro 300.000 annui per ciascuno degli anni 2025 e 2026 per la realizzazione di progetti sperimentali volti all'applicazione dell'intelligenza artificiale ai servizi forniti dal Ministero degli affari esteri e della cooperazione internazionale a cittadini e imprese.

2. Agli oneri derivanti dal comma 1, pari a euro 300.000 annui per ciascuno degli anni 2025 e 2026, si provvede mediante corrispondente riduzione dello stanziamento del fondo speciale di parte corrente iscritto, ai fini del bilancio triennale 2025-2027, nell'ambito del programma «Fondi di riserva e speciali» della missione «Fondi da ripartire» dello stato di previsione del Ministero dell'economia e delle finanze per l'anno 2025, allo scopo parzialmente utilizzando l'accantonamento relativo al Ministero degli affari esteri e della cooperazione internazionale.

Art. 22.

Misure di sostegno ai giovani e allo sport

1. All'articolo 5, comma 1, lettera d), del decreto legislativo 27 dicembre 2023, n. 209, sono aggiunte, in fine, le seguenti parole: «, oppure hanno svolto un'attività di ricerca anche applicata nell'ambito delle tecnologie di intelligenza artificiale».



2. Nel piano didattico personalizzato (PDP) adottato dall'istituzione scolastica secondaria di secondo grado nell'ambito della propria autonomia, per le studentesse e gli studenti ad alto potenziale cognitivo possono essere inserite attività volte all'acquisizione di ulteriori competenze attraverso esperienze di apprendimento presso le istituzioni della formazione superiore, in deroga a quanto previsto dall'articolo 6 del regolamento di cui al decreto del Ministro dell'istruzione, dell'università e della ricerca 22 ottobre 2004, n. 270, in materia di previo possesso del titolo, in coerenza con il profilo in uscita dell'indirizzo di studio. I crediti formativi acquisiti nell'ambito delle attività di cui al primo periodo sono valutati nell'ambito dei percorsi formativi della formazione superiore intrapresi dopo il conseguimento del titolo di cui al medesimo primo periodo.

3. Lo Stato favorisce l'accessibilità ai sistemi di intelligenza artificiale per il miglioramento del benessere psico-fisico attraverso l'attività sportiva, anche ai fini dello sviluppo di soluzioni innovative finalizzate a una maggiore inclusione in ambito sportivo delle persone con disabilità. Nel rispetto dei principi generali di cui alla presente legge, i sistemi di intelligenza artificiale possono essere utilizzati anche per l'organizzazione delle attività sportive.

Art. 23.

Investimenti nei settori dell'intelligenza artificiale, della cybersicurezza e del calcolo quantistico

1. In linea con la strategia nazionale di cui all'articolo 19, al fine di supportare lo sviluppo di imprese operanti nei settori dell'intelligenza artificiale e della cybersicurezza e delle tecnologie per essi abilitanti, ivi compresi le tecnologie quantistiche e i sistemi di telecomunicazioni, anche tramite la creazione di poli di trasferimento tecnologico e programmi di accelerazione operanti nei medesimi settori, avvalendosi dell'operatività della società di gestione del risparmio di cui all'articolo 1, comma 116, della legge 30 dicembre 2018, n. 145, è autorizzato, fino all'ammontare complessivo di un miliardo di euro, l'investimento, sotto forma di *equity* e *quasi equity*, nel capitale di rischio direttamente o indirettamente di:

a) piccole e medie imprese (PMI) con elevato potenziale di sviluppo e innovative, aventi sede operativa in Italia, che operano nei settori dell'intelligenza artificiale e della cybersicurezza e delle tecnologie per essi abilitanti, ivi compresi le tecnologie quantistiche e i sistemi di telecomunicazioni, con particolare riferimento al 5G e alle sue evoluzioni, al *mobile edge computing*, alle architetture aperte basate su soluzioni *software*, al *Web 3*, all'elaborazione del segnale, anche in relazione ai profili di sicurezza e integrità delle reti di comunicazione elettroniche, e che si trovano in fase di sperimentazione (*seed financing*), di costituzione (*start up financing*), di avvio dell'attività (*early-stage financing*) o di sviluppo del prodotto (*expansion, scale up financing*);

b) imprese, aventi sede operativa in Italia, anche diverse da quelle di cui alla lettera a), operanti nei settori e nelle tecnologie di cui alla medesima lettera a), con elevato potenziale di sviluppo e altamente innovative, al fine di promuoverne lo sviluppo come campioni tecnologici nazionali.

2. Gli investimenti di cui al comma 1 sono effettuati mediante utilizzo delle risorse del Fondo di sostegno al *venture capital* di cui all'articolo 1, comma 209, della legge 30 dicembre 2018, n. 145, secondo le disposizioni di cui al decreto del Ministro dello sviluppo economico 27 giugno 2019, pubblicato nella *Gazzetta Ufficiale* n. 176 del 29 luglio 2019, sia mediante la sottoscrizione, direttamente o indirettamente, di quote o azioni di uno o più fondi per il *venture capital* appositamente istituiti e gestiti dalla società di gestione del risparmio di cui al comma 1, sia mediante coinvestimento da parte di altri fondi per il *venture capital* istituiti e gestiti dalla medesima società di gestione del risparmio. La normativa di attuazione di cui al citato decreto del Ministro dello sviluppo economico 27 giugno 2019 è aggiornata alle disposizioni del presente articolo, con adeguamento per gli investimenti nelle imprese di cui al comma 1, lettera b), non rientranti nella definizione di PMI.

3. Oltre al Ministero delle imprese e del made in Italy in qualità di investitore, partecipano con propri rappresentanti agli organi di governo dei fondi di *venture capital* di cui al presente articolo, in ragione delle proprie competenze, la struttura della Presidenza del Consiglio dei ministri competente in materia di innovazione tecnologica e transizione digitale e l'Agenzia per la cybersicurezza nazionale, in ogni caso senza compensi o indennità.

Art. 24.

Deleghe al Governo in materia di intelligenza artificiale

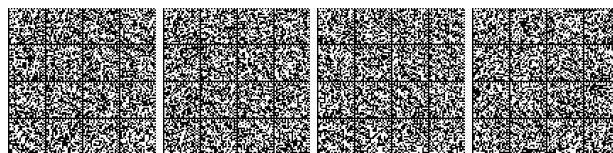
1. Il Governo è delegato ad adottare, entro dodici mesi dalla data di entrata in vigore della presente legge, con le procedure di cui all'articolo 31 della legge 24 dicembre 2012, n. 234, acquisiti i pareri delle competenti Commissioni parlamentari, della Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, e del Garante per la protezione dei dati personali, uno o più decreti legislativi per l'adeguamento della normativa nazionale al regolamento (UE) 2024/1689.

2. Nell'esercizio della delega di cui al comma 1 il Governo si attiene, oltre che ai principi e criteri direttivi generali di cui all'articolo 32 della legge 24 dicembre 2012, n. 234, ai seguenti principi e criteri direttivi specifici:

a) attribuire alle autorità di cui all'articolo 20, nei limiti della designazione operata ai sensi del medesimo articolo 20, tutti i poteri di vigilanza, ispettivi e sanzionatori previsti dal regolamento (UE) 2024/1689 per la verifica del rispetto delle norme del regolamento stesso e dalla normativa dell'Unione europea attuativa del medesimo regolamento;

b) apportare alla normativa vigente, ivi inclusa quella in materia di servizi bancari, finanziari, assicurativi e di pagamento, le modifiche, le integrazioni e le abrogazioni necessarie al corretto e integrale adeguamento al regolamento (UE) 2024/1689;

c) ricorrere alla disciplina secondaria adottata dalle autorità individuate ai sensi dell'articolo 20, ove opportuno e nel rispetto delle competenze alle stesse spettanti, nell'ambito e per le finalità specificamente previsti dal regolamento (UE) 2024/1689 e dalla normativa dell'Unione europea attuativa del medesimo regolamento;



d) attribuire alle autorità di cui all'articolo 20 il potere di imporre le sanzioni e le altre misure amministrative previste dall'articolo 99 del regolamento (UE) 2024/1689 per la violazione delle norme del regolamento stesso e degli atti di attuazione, nel rispetto dei limiti edittali e delle procedure previsti dal medesimo articolo 99 e dalle disposizioni nazionali che disciplinano l'irrogazione delle sanzioni e l'applicazione delle altre misure amministrative da parte delle autorità anzidette;

e) previsione di percorsi di alfabetizzazione e formazione in materia di utilizzo dei sistemi di intelligenza artificiale;

f) previsione, da parte degli ordini professionali e delle associazioni di categoria maggiormente rappresentative, nonché da parte delle forme aggregative delle associazioni di cui all'articolo 3 della legge 14 gennaio 2013, n. 4, di percorsi di alfabetizzazione e formazione, per i professionisti e per gli operatori dello specifico settore, all'uso dei sistemi di intelligenza artificiale; previsione della possibilità di riconoscimento di un equo compenso modulabile sulla base delle responsabilità e dei rischi connessi all'uso dei sistemi di intelligenza artificiale;

g) potenziamento, all'interno dei curricula scolastici, dello sviluppo di competenze scientifiche, tecnologiche, ingegneristiche e matematiche legate alle discipline STEM, nonché artistiche, al fine di promuovere la scelta da parte delle studentesse e degli studenti, anche attraverso mirate attività di orientamento personalizzato, di percorsi di formazione superiore relativi alle menzionate discipline;

h) previsione di un'apposita disciplina per l'utilizzo di sistemi di intelligenza artificiale per l'attività di polizia;

i) previsione, nei corsi universitari e delle istituzioni di alta formazione artistica, musicale e coreutica (AFAM), nonché nei percorsi di istruzione tecnologica superiore offerti dagli istituti tecnologici superiori (ITS *Academy*), coerentemente con i rispettivi profili culturali e professionali, di attività formative per la comprensione tecnica e l'utilizzo consapevole anche sotto il profilo giuridico delle tecnologie, anche con riferimento ai sistemi di intelligenza artificiale come definiti dalla disciplina europea, nonché per la corretta interpretazione della produzione di tali sistemi in termini di previsioni, contenuti, raccomandazioni o decisioni;

l) valorizzazione delle attività di ricerca e di trasferimento tecnologico in materia di intelligenza artificiale svolte da università, istituzioni AFAM, ITS *Academy* ed enti pubblici di ricerca, mediante disposizioni finalizzate al perseguimento dei seguenti obiettivi:

1) agevolare il coinvolgimento del sistema dell'università e della ricerca nella promozione, nella realizzazione e nell'utilizzo di spazi di sperimentazione normativa in collaborazione con il mondo produttivo;

2) incentivare le attività di supporto e semplificare gli strumenti di collaborazione tra il sistema dell'università e della ricerca e degli ITS *Academy* e le Autorità nazionali di cui all'articolo 20;

m) definizione dei poteri di vigilanza dell'autorità di vigilanza del mercato che conferiscano all'autorità i poteri di imporre ai fornitori e ai potenziali fornitori di tra-

smettere informazioni, di effettuare ispezioni a distanza o *in loco*, anche senza preavviso, e di svolgere controlli sulla conduzione delle prove in condizioni reali e sui relativi sistemi di intelligenza artificiale ad alto rischio;

n) adeguamento del quadro sanzionatorio, anche in deroga ai criteri e ai limiti previsti dall'articolo 32, comma 1, lettera d), della legge 24 dicembre 2012, n. 234, e alla legge 24 novembre 1981, n. 689, ivi compresa la definizione delle misure di esecuzione applicabili ai sensi del regolamento (UE) 2024/1689, nonché del procedimento applicabile per l'irrogazione delle sanzioni o l'applicazione delle misure di esecuzione, anche in coerenza con quanto previsto dall'articolo 17, comma 4-*quater*, del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109.

3. Il Governo è altresì delegato ad adottare, entro dodici mesi dalla data di entrata in vigore della presente legge, uno o più decreti legislativi per adeguare e specificare la disciplina dei casi di realizzazione e di impiego illeciti di sistemi di intelligenza artificiale.

4. Gli schemi dei decreti legislativi di cui al comma 3 sono adottati su proposta del Presidente del Consiglio dei ministri e del Ministro della giustizia, di concerto con il Ministro dell'interno, e sono successivamente trasmessi alle Camere per l'espressione del parere delle Commissioni parlamentari competenti. Decorsi sessanta giorni dalla data della trasmissione, i decreti possono essere emanati anche in mancanza dei pareri. Qualora detto termine venga a scadere nei trenta giorni antecedenti alla scadenza del termine previsto per l'esercizio della delega o successivamente, quest'ultimo è prorogato di sessanta giorni.

5. Nell'esercizio della delega di cui al comma 3, il Governo si attiene ai seguenti principi e criteri direttivi:

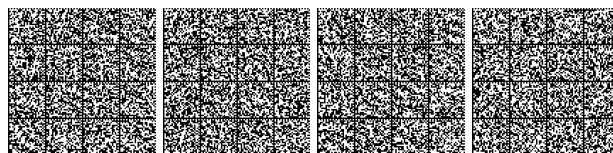
a) previsione di strumenti, anche cautelari, finalizzati a inibire la diffusione e a rimuovere contenuti generati illecitamente anche con sistemi di intelligenza artificiale, assistiti da un sistema di sanzioni effettive, proporzionate e dissuasive;

b) introduzione di autonome fattispecie di reato, punite a titolo di dolo o di colpa, incentrate sull'omessa adozione o sull'omesso adeguamento di misure di sicurezza per la produzione, la messa in circolazione e l'utilizzo professionale di sistemi di intelligenza artificiale, quando da tali omissioni deriva pericolo concreto per la vita o l'incolumità pubblica o individuale o per la sicurezza dello Stato;

c) precisazione dei criteri di imputazione della responsabilità penale delle persone fisiche e amministrativa degli enti per gli illeciti inerenti a sistemi di intelligenza artificiale, che tenga conto del livello effettivo di controllo dei sistemi predetti da parte dell'agente;

d) nei casi di responsabilità civile, previsione di strumenti di tutela del danneggiato, anche attraverso una specifica regolamentazione dei criteri di ripartizione dell'onere della prova, tenuto conto della classificazione dei sistemi di intelligenza artificiale e dei relativi obblighi come individuati dal regolamento (UE) 2024/1689;

e) regolazione dell'utilizzo dei sistemi di intelligenza artificiale nelle indagini preliminari, nel rispetto delle



garanzie inerenti al diritto di difesa e ai dati personali dei terzi, nonché dei principi di proporzionalità, non discriminazione e trasparenza;

f) modifica, a fini di coordinamento e di razionalizzazione del sistema, della normativa sostanziale e processuale vigente, in conformità ai principi e ai criteri enunciati nelle lettere a), b), c), d) ed e).

6. Dall'attuazione del presente articolo non devono derivare nuovi o maggiori oneri a carico della finanza pubblica. Le amministrazioni competenti provvedono ai relativi adempimenti con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente.

Capo IV

DISPOSIZIONI A TUTELA DEGLI UTENTI E IN MATERIA DI DIRITTO D'AUTORE

Art. 25.

Tutela del diritto d'autore delle opere generate con l'ausilio dell'intelligenza artificiale

1. Alla legge 22 aprile 1941, n. 633, sono apportate le seguenti modificazioni:

a) all'articolo 1, primo comma, dopo le parole: «opere dell'ingegno» è inserita la seguente: «umano» e dopo le parole: «forma di espressione» sono aggiunte le seguenti: «, anche laddove create con l'ausilio di strumenti di intelligenza artificiale, purché costituenti risultato del lavoro intellettuale dell'autore»;

b) dopo l'articolo 70-sexies è inserito il seguente:

«Art. 70-septies. — 1. Fermo restando quanto previsto dalla Convenzione di Berna per la protezione delle opere letterarie ed artistiche, ratificata e resa esecutiva ai sensi della legge 20 giugno 1978, n. 399, le riproduzioni e le estrazioni da opere o da altri materiali contenuti in rete o in banche di dati a cui si ha legittimamente accesso, ai fini dell'estrazione di testo e di dati attraverso modelli e sistemi di intelligenza artificiale, anche generativa, sono consentite in conformità alle disposizioni di cui agli articoli 70-ter e 70-quater».

Capo V

DISPOSIZIONI PENALI

Art. 26.

Modifiche al codice penale e ad ulteriori disposizioni penali

1. Al codice penale sono apportate le seguenti modificazioni:

a) all'articolo 61, dopo il numero 11-novies) è aggiunto il seguente:

«11-decies) l'avere commesso il fatto mediante l'impiego di sistemi di intelligenza artificiale, quando gli stessi, per la loro natura o per le modalità di utilizzo, abbiano costituito mezzo insidioso, ovvero quando il loro impiego abbia comunque ostacolato la pubblica o la privata difesa, ovvero aggravato le conseguenze del reato»;

b) all'articolo 294 è aggiunto, in fine, il seguente comma:

«La pena è della reclusione da due a sei anni se l'inganno è posto in essere mediante l'impiego di sistemi di intelligenza artificiale»;

c) dopo l'articolo 612-ter è inserito il seguente:

«Art. 612-quater (*Illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale*).

— Chiunque cagiona un danno ingiusto ad una persona, cedendo, pubblicando o altrimenti diffondendo, senza il suo consenso, immagini, video o voci falsificati o alterati mediante l'impiego di sistemi di intelligenza artificiale e idonei a indurre in inganno sulla loro genuinità, è punito con la reclusione da uno a cinque anni. Il delitto è punibile a querela della persona offesa. Si procede tuttavia d'ufficio se il fatto è connesso con altro delitto per il quale si deve procedere d'ufficio ovvero se è commesso nei confronti di persona incapace, per età o per infermità, o di una pubblica autorità a causa delle funzioni esercitate».

2. All'articolo 2637 del codice civile è aggiunto, in fine, il seguente periodo: «La pena è della reclusione da due a sette anni se il fatto è commesso mediante l'impiego di sistemi di intelligenza artificiale».

3. All'articolo 171, primo comma, della legge 22 aprile 1941, n. 633, dopo la lettera a-bis) è inserita la seguente:

«a-ter) riproduce o estrae testo o dati da opere o altri materiali disponibili in rete o in banche di dati in violazione degli articoli 70-ter e 70-quater, anche attraverso sistemi di intelligenza artificiale».

4. All'articolo 185, comma 1, del testo unico delle disposizioni in materia di intermediazione finanziaria, di cui al decreto legislativo 24 febbraio 1998, n. 58, è aggiunto, in fine, il seguente periodo: «La pena è della reclusione da due a sette anni e della multa da euro venticinquemila a euro sei milioni se il fatto è commesso mediante l'impiego di sistemi di intelligenza artificiale».

Capo VI

DISPOSIZIONI FINANZIARIE E FINALI

Art. 27.

Clausola di invarianza finanziaria

1. Dall'attuazione della presente legge, ad esclusione dell'articolo 21, non devono derivare nuovi o maggiori oneri a carico della finanza pubblica. Le amministrazioni pubbliche interessate provvedono all'adempimento delle disposizioni della presente legge con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente.

Art. 28.

Disposizioni finali

1. All'articolo 7, comma 1, del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, la lettera z) è sostituita dalla seguente:

«z) per le finalità di cui al presente articolo, può concludere accordi di collaborazione, comunque denominati, con soggetti privati, costituire e partecipare a partenariati



pubblico-privato nel territorio nazionale, nonché, previa autorizzazione del Presidente del Consiglio dei ministri, a consorzi, fondazioni o società con soggetti pubblici e privati, italiani o di Paesi appartenenti all'Unione europea. Sulla base dell'interesse nazionale e previa autorizzazione del Presidente del Consiglio dei ministri, può altresì partecipare a consorzi, fondazioni o società con soggetti pubblici e privati di Paesi della NATO ovvero di Paesi extraeuropei con i quali siano stati sottoscritti accordi di cooperazione o di partenariato per lo sviluppo di sistemi di intelligenza artificiale».

2. Alla legge 28 giugno 2024, n. 90, sono apportate le seguenti modificazioni:

a) all'articolo 1, comma 1, le parole: «di cui all'articolo 1, comma 3-bis, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, come modificato dall'articolo 3 della presente legge» sono sostituite dalle seguenti: «adottata con determinazione tecnica del direttore generale dell'Agenzia per la cybersicurezza nazionale»;

b) nel capo I, dopo l'articolo 15 è aggiunto il seguente:

«Art. 15-bis (*Disposizioni di coordinamento*).
— 1. Ogni riferimento al decreto legislativo 18 maggio 2018, n. 65, è da intendersi alle corrispondenti disposizioni di cui al decreto legislativo 4 settembre 2024, n. 138, a decorrere dalla data in cui le stesse acquistano efficacia».

La presente legge, munita del sigillo dello Stato, sarà inserita nella Raccolta ufficiale degli atti normativi della Repubblica italiana. È fatto obbligo a chiunque spetti di osservarla e di farla osservare come legge dello Stato.

Data a Roma, addì 23 settembre 2025

MATTARELLA

MELONI, *Presidente del Consiglio dei ministri*

NORDIO, *Ministro della giustizia*

Visto, il Guardasigilli: NORDIO

LAVORI PREPARATORI

Senato della Repubblica (atto n. 1146):

Presentato dal Presidente del Consiglio GIORGIA MELONI e dal Ministro della giustizia CARLO NORDIO (Governo MELONI-I), il 20 maggio 2024.

Assegnato alle Commissioni riunite 8^a (Ambiente, transizione ecologica, energia, lavori pubblici, comunicazioni, innovazione tecnologica) e 10^a (Affari sociali, sanità, lavoro pubblico e privato, previdenza sociale), in sede referente, il 29 maggio 2024, con i pareri delle Commissioni 1^a (Affari costituzionali, affari della Presidenza del Consiglio e dell'Interno, ordinamento generale dello Stato e della pubblica amministrazione, editoria, digitalizzazione), 2^a (Giustizia), 3^a (Affari esteri e difesa), 4^a (Politiche dell'Unione europea), 5^a (Programmazione economica, bilancio), 6^a (Finanze e tesoro), 7^a (Cultura e patrimonio culturale, istruzione pubblica, ricerca scientifica, spettacolo e sport) e 9^a Commissione (Industria, commercio, turismo, agricoltura e produzione agroalimentare).

Esaminato dalle Commissioni riunite 8^a (Ambiente, transizione ecologica, energia, lavori pubblici, comunicazioni, innovazione tecnologica) e 10^a (Affari sociali, sanità, lavoro pubblico e privato, previdenza sociale), in sede referente, l'11 e il 13 giugno 2024; il 22 e il 29 ottobre 2024; il 12, il 20 e il 27 novembre 2024; l'11, il 12, il 18 e il 19 marzo 2025.

Esaminato in Aula il 19 marzo 2025 e approvato il 20 marzo 2025.

Camera dei deputati (atto n. 2316):

Assegnato alle Commissioni riunite X (Attività produttive, commercio e turismo) e IX (Trasporti, poste e telecomunicazioni), in sede referente, il 24 marzo 2025, con i pareri delle Commissioni I (Affari costituzionali, della Presidenza del Consiglio e interni), II (Giustizia), III (Affari esteri e comunitari), IV (Difesa), V (Bilancio, tesoro e programmazione), VI (Finanze), VII (Cultura, scienza e istruzione), XI (Lavoro pubblico e privato), XII (Affari sociali), XIV (Politiche dell'unione europea) e per le Questioni regionali.

Esaminato dalle Commissioni riunite X (Attività produttive, commercio e turismo) e IX (Trasporti, poste e telecomunicazioni), in sede referente, il 16 aprile 2025; il 20, il 27 e il 28 maggio 2025; il 12 e il 17 giugno 2025.

Esaminato in Aula il 23 e il 24 giugno 2025 e approvato, con modificazioni, il 25 giugno 2025.

Senato della Repubblica (atto n. 1146-B):

Nuovamente assegnato alle Commissioni riunite 8^a (Ambiente, transizione ecologica, energia, lavori pubblici, comunicazioni, innovazione tecnologica) e 10^a (Affari sociali, sanità, lavoro pubblico e privato, previdenza sociale), in sede referente, il 2 luglio 2025, con i pareri delle Commissioni 1^a (Affari costituzionali, affari della Presidenza del Consiglio e dell'Interno, ordinamento generale dello Stato e della Pubblica Amministrazione, editoria, digitalizzazione), 2^a (Giustizia), 3^a (Affari esteri e difesa), 4^a (Politiche dell'Unione europea), 5^a (Programmazione economica, bilancio), 7^a (Cultura e patrimonio culturale, istruzione pubblica, ricerca scientifica, spettacolo e sport) e 9^a Commissione (Industria, commercio, turismo, agricoltura e produzione agroalimentare).

Esaminato dalle Commissioni riunite 8^a (Ambiente, transizione ecologica, energia, lavori pubblici, comunicazioni, innovazione tecnologica) e 10^a (Affari sociali, sanità, lavoro pubblico e privato, previdenza sociale), in sede referente, il 9, il 16, il 23 e il 30 luglio 2025.

Esaminato in Aula e approvato, definitivamente, il 17 settembre 2025.

NOTE

AVVERTENZA:

Il testo delle note qui pubblicato è stato redatto dall'amministrazione competente per materia ai sensi dell'articolo 10, commi 2 e 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 gli atti dell'Unione europea vengono forniti gli estremi di pubblicazione nella Gazzetta Ufficiale dell'Unione Europea (GUUE).

Note all'art. 1:

— Il regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale) è pubblicato nella GUUE, del 12 luglio 2024.



Note all'art. 2:

— Per i riferimenti al regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024 si vedano le note all'articolo 1.

Note all'art. 3:

— La legge 3 marzo 2009, n. 1 recante: «Ratifica ed esecuzione della Convenzione delle Nazioni Unite sui diritti delle persone con disabilità, con Protocollo opzionale, fatta a New York il 13 dicembre 2006 e istituzione dell'Osservatorio nazionale sulla condizione delle persone con disabilità» è pubblicata nella *Gazzetta Ufficiale* n. 61 del 14 marzo 2009.

Note all'art. 4:

— Il Regolamento (UE) 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 (regolamento generale sulla protezione dei dati) è pubblicato GUUE del 4 maggio 2016, n. L119.

— Il decreto legislativo 30 giugno 2003, n. 196, recante: «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» è pubblicato nella *Gazzetta Ufficiale* n. 174 del 29 luglio 2003, S.O. n. 123.

Note all'art. 5:

— Si riporta il testo dell'articolo 1 del decreto legislativo 30 marzo 2001, n. 165, recante: «Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche», pubblicato nella *Gazzetta Ufficiale* n. 106 del 9 maggio 2001:

«Art. 1 (*Finalità ed ambito di applicazione*). — 1. Le disposizioni del presente decreto disciplinano l'organizzazione degli uffici e i rapporti di lavoro e di impiego alle dipendenze delle amministrazioni pubbliche, tenuto conto delle autonomie locali e di quelle delle regioni e delle province autonome, nel rispetto dell'articolo 97, comma primo, della Costituzione, al fine di:

a) accrescere l'efficienza delle amministrazioni in relazione a quella dei corrispondenti uffici e servizi dei Paesi dell'Unione europea, anche mediante il coordinato sviluppo di sistemi informativi pubblici;

b) razionalizzare il costo del lavoro pubblico, contenendo la spesa complessiva per il personale, diretta e indiretta, entro i vincoli di finanza pubblica;

c) realizzare la migliore utilizzazione delle risorse umane nelle pubbliche amministrazioni, assicurando la formazione e lo sviluppo professionale dei dipendenti, applicando condizioni uniformi rispetto a quelle del lavoro privato, garantendo pari opportunità alle lavoratrici ed ai lavoratori nonché l'assenza di qualunque forma di discriminazione e di violenza morale o psichica.

2. Per amministrazioni pubbliche si intendono tutte le amministrazioni dello Stato, ivi compresi gli istituti e scuole di ogni ordine e grado e le istituzioni educative, le aziende ed amministrazioni dello Stato ad ordinamento autonomo, le Regioni, le Province, i Comuni, le Comunità montane, e loro consorzi e associazioni, le istituzioni universitarie, gli Istituti autonomi case popolari, le Camere di commercio, industria, artigianato e agricoltura e loro associazioni, tutti gli enti pubblici non economici nazionali, regionali e locali, le amministrazioni, le aziende e gli enti del Servizio sanitario nazionale, l'Agenzia per la rappresentanza negoziale delle pubbliche amministrazioni (ARAN) e le Agenzie di cui al decreto legislativo 30 luglio 1999, n. 300. Fino alla revisione organica della disciplina di settore, le disposizioni di cui al presente decreto continuano ad applicarsi anche al CONI.

3. Le disposizioni del presente decreto costituiscono principi fondamentali ai sensi dell'articolo 117 della Costituzione. Le Regioni a statuto ordinario si attengono ad esse tenendo conto delle peculiarità dei rispettivi ordinamenti. I principi desumibili dall'articolo 2 della legge 23 ottobre 1992, n. 421, e successive modificazioni, e dall'articolo 11, comma 4, della legge 15 marzo 1997, n. 59, e successive modificazioni ed integrazioni, costituiscono altresì, per le Regioni a statuto speciale e per le province autonome di Trento e di Bolzano, norme fondamentali di riforma economico-sociale della Repubblica.».

Note all'art. 6:

— Si riporta il testo degli articoli 4, 6, 7, 11 e 13 della legge 3 agosto 2007, n. 124, recante: «Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto», pubblicato nella *Gazzetta Ufficiale* n. 187 del 13 agosto 2007:

«Art. 4 (*Dipartimento delle informazioni per la sicurezza*). — 1. Per lo svolgimento dei compiti di cui al comma 3 è istituito, presso la Presidenza del Consiglio dei ministri, il Dipartimento delle informazioni per la sicurezza (DIS).

2. Il Presidente del Consiglio dei ministri e l'Autorità delegata, ove istituita, si avvalgono del DIS per l'esercizio delle loro competenze, al fine di assicurare piena unitarietà nella programmazione della ricerca informativa del Sistema di informazione per la sicurezza, nonché nelle analisi e nelle attività operative dei servizi di informazione per la sicurezza.

3. Il DIS svolge i seguenti compiti:

a) coordina l'intera attività di informazione per la sicurezza, verificando altresì i risultati delle attività svolte dall'AISE e dall'AISI, ferma restando la competenza dei predetti servizi relativamente alle attività di ricerca informativa e di collaborazione con i servizi di sicurezza degli Stati esteri;

b) è costantemente informato delle operazioni di competenza dei servizi di informazione per la sicurezza e trasmette al Presidente del Consiglio dei ministri le informative e le analisi prodotte dal Sistema di informazione per la sicurezza;

c) raccoglie le informazioni, le analisi e i rapporti provenienti dai servizi di informazione per la sicurezza, dalle Forze armate e di polizia, dalle amministrazioni dello Stato e da enti di ricerca anche privati; ferma l'esclusiva competenza dell'AISE e dell'AISI per l'elaborazione dei rispettivi piani di ricerca operativa, elabora analisi strategiche o relative a particolari situazioni; formula valutazioni e previsioni, sulla scorta dei contributi analitici settoriali dell'AISE e dell'AISI;

d) elabora, anche sulla base delle informazioni e dei rapporti di cui alla lettera c), analisi globali da sottoporre al CISR, nonché progetti di ricerca informativa, sui quali decide il Presidente del Consiglio dei ministri, dopo avere acquisito il parere del CISR;

d-bis) sulla base delle direttive di cui all'articolo 1, comma 3-bis, nonché delle informazioni e dei rapporti di cui alla lettera c) del presente comma, coordina le attività di ricerca informativa finalizzate a rafforzare la protezione cibernetica e la sicurezza informatica nazionali;

e) promuove e garantisce, anche attraverso riunioni periodiche, lo scambio informativo tra l'AISE, l'AISI e le Forze di polizia; comunica al Presidente del Consiglio dei ministri le acquisizioni provenienti dallo scambio informativo e i risultati delle riunioni periodiche;

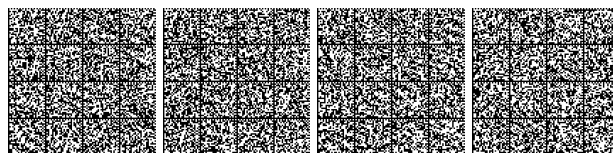
f) trasmette, su disposizione del Presidente del Consiglio dei ministri, sentito il CISR, informazioni e analisi ad amministrazioni pubbliche o enti, anche ad ordinamento autonomo, interessati all'acquisizione di informazioni per la sicurezza;

g) elabora, d'intesa con l'AISE e l'AISI, il piano di acquisizione delle risorse umane e materiali e di ogni altra risorsa comunque strumentale all'attività dei servizi di informazione per la sicurezza, da sottoporre all'approvazione del Presidente del Consiglio dei ministri;

h) sentite l'AISE e l'AISI, elabora e sottopone all'approvazione del Presidente del Consiglio dei ministri lo schema del regolamento di cui all'articolo 21, comma 1;

i) esercita il controllo sull'AISE e sull'AISI, verificando la conformità delle attività di informazione per la sicurezza alle leggi e ai regolamenti, nonché alle direttive e alle disposizioni del Presidente del Consiglio dei ministri. Per tale finalità, presso il DIS è istituito un ufficio ispettivo le cui modalità di organizzazione e di funzionamento sono definite con il regolamento di cui al comma 7. Con le modalità previste da tale regolamento è approvato annualmente, previo parere del Comitato parlamentare di cui all'articolo 30, il piano annuale delle attività dell'ufficio ispettivo. L'ufficio ispettivo, nell'ambito delle competenze definite con il predetto regolamento, può svolgere, anche a richiesta del direttore generale del DIS, autorizzato dal Presidente del Consiglio dei ministri, inchieste interne su specifici episodi e comportamenti verificatisi nell'ambito dei servizi di informazione per la sicurezza;

l) assicura l'attuazione delle disposizioni impartite dal Presidente del Consiglio dei Ministri con apposito regolamento adottato ai sensi dell'articolo 1, comma 2, ai fini della tutela amministrativa del segreto di Stato e delle classifiche di segretezza, vigilando altresì sulla loro corretta applicazione;



m) cura le attività di promozione e diffusione della cultura della sicurezza e la comunicazione istituzionale;

n) impartisce gli indirizzi per la gestione unitaria del personale di cui all'articolo 21, secondo le modalità definite dal regolamento di cui al comma 1 del medesimo articolo;

n-bis) gestisce unitariamente, ferme restando le competenze operative dell'AISE e dell'AISI, gli approvvigionamenti e i servizi logistici comuni.

4. Fermo restando quanto previsto dall'articolo 118-bis del codice di procedura penale, introdotto dall'articolo 14 della presente legge, qualora le informazioni richieste alle Forze di polizia, ai sensi delle lettere c) ed e) del comma 3 del presente articolo, siano relative a indagini di polizia giudiziaria, le stesse, se coperte dal segreto di cui all'articolo 329 del codice di procedura penale, possono essere acquisite solo previo nulla osta della autorità giudiziaria competente. L'autorità giudiziaria può trasmettere gli atti e le informazioni anche di propria iniziativa.

5. La direzione generale del DIS è affidata ad un dirigente di prima fascia o equiparato dell'amministrazione dello Stato, la cui nomina e revoca spettano in via esclusiva al Presidente del Consiglio dei ministri, sentito il CISR. L'incarico ha la durata massima di otto anni ed è conferibile, senza soluzione di continuità, anche con provvedimenti successivi, ciascuno dei quali di durata non superiore al quadriennio. Per quanto previsto dalla presente legge, il direttore del DIS è il diretto referente del Presidente del Consiglio dei ministri e dell'Autorità delegata, ove istituita, salvo quanto previsto dall'articolo 6, comma 5, e dall'articolo 7, comma 5, ed è gerarchicamente e funzionalmente sovraordinato al personale del DIS e degli uffici istituiti nell'ambito del medesimo Dipartimento.

6. Il Presidente del Consiglio dei ministri, sentito il direttore generale del DIS, nomina uno o più vicedirettori generali; il direttore generale affida gli altri incarichi nell'ambito del Dipartimento, ad eccezione degli incarichi il cui conferimento spetta al Presidente del Consiglio dei ministri.

7. L'ordinamento e l'organizzazione del DIS e degli uffici istituiti nell'ambito del medesimo Dipartimento sono disciplinati con apposito regolamento.

8. Il regolamento previsto dal comma 7 definisce le modalità di organizzazione e di funzionamento dell'ufficio ispettivo di cui al comma 3, lettera i), secondo i seguenti criteri:

a) agli ispettori è garantita piena autonomia e indipendenza di giudizio nell'esercizio delle funzioni di controllo;

b) salva specifica autorizzazione del Presidente del Consiglio dei ministri o dell'Autorità delegata, ove istituita, i controlli non devono interferire con le operazioni in corso;

c) sono previste per gli ispettori specifiche prove selettive e un'adeguata formazione;

d) non è consentito il passaggio di personale dall'ufficio ispettivo ai servizi di informazione per la sicurezza;

e) gli ispettori, previa autorizzazione del Presidente del Consiglio dei ministri o dell'Autorità delegata, ove istituita, possono accedere a tutti gli atti conservati presso i servizi di informazione per la sicurezza e presso il DIS; possono altresì acquisire, tramite il direttore generale del DIS, altre informazioni da enti pubblici e privati».

«Art. 6 (Agenzia informazioni e sicurezza esterna). — 1. È istituita l'Agenzia informazioni e sicurezza esterna (AISE), alla quale è affidato il compito di ricercare ed elaborare nei settori di competenza tutte le informazioni utili alla difesa dell'indipendenza, dell'integrità e della sicurezza della Repubblica, anche in attuazione di accordi internazionali, dalle minacce provenienti dall'estero.

2. Spettano all'AISE, inoltre, le attività in materia di controproliferazione concernenti i materiali strategici, nonché le attività di informazione per la sicurezza, che si svolgono al di fuori del territorio nazionale, a protezione degli interessi politici, militari, economici, scientifici e industriali dell'Italia.

3. È, altresì, compito dell'AISE individuare e contrastare al di fuori del territorio nazionale le attività di spionaggio dirette contro l'Italia e le attività volte a danneggiare gli interessi nazionali.

4. L'AISE può svolgere operazioni sul territorio nazionale soltanto in collaborazione con l'AISI, quando tali operazioni siano strettamente connesse ad attività che la stessa AISE svolge all'estero. A tal fine il direttore generale del DIS provvede ad assicurare le necessarie forme di coordinamento e di raccordo informativo, anche al fine di evitare sovrapposizioni funzionali o territoriali.

5. L'AISE risponde al Presidente del Consiglio dei ministri.

6. L'AISE informa tempestivamente e con continuità il Ministro della difesa, il Ministro degli affari esteri e il Ministro dell'interno per i profili di rispettiva competenza.

7. Il Presidente del Consiglio dei ministri, con proprio decreto, nomina e revoca il direttore dell'AISE, scelto tra dirigenti di prima fascia o equiparati dell'amministrazione dello Stato, sentito il CISR. L'incarico ha la durata massima di otto anni ed è conferibile, senza soluzione di continuità, anche con provvedimenti successivi, ciascuno dei quali di durata non superiore al quadriennio.

8. Il direttore dell'AISE riferisce costantemente sull'attività svolta al Presidente del Consiglio dei ministri o all'Autorità delegata, ove istituita, per il tramite del direttore generale del DIS. Riferisce direttamente al Presidente del Consiglio dei ministri in caso di urgenza o quando altre particolari circostanze lo richiedano, informandone senza ritardo il direttore generale del DIS; presenta al CISR, per il tramite del direttore generale del DIS, un rapporto annuale sul funzionamento e sull'organizzazione dell'Agenzia.

9. Il Presidente del Consiglio dei ministri nomina e revoca, sentito il direttore dell'AISE, uno o più vicedirettori. Il direttore dell'AISE affida gli altri incarichi nell'ambito dell'Agenzia.

10. L'organizzazione e il funzionamento dell'AISE sono disciplinati con apposito regolamento.

Art. 7 (Agenzia informazioni e sicurezza interna). — 1. È istituita l'Agenzia informazioni e sicurezza interna (AISI), alla quale è affidato il compito di ricercare ed elaborare nei settori di competenza tutte le informazioni utili a difendere, anche in attuazione di accordi internazionali, la sicurezza interna della Repubblica e le istituzioni democratiche poste dalla Costituzione a suo fondamento da ogni minaccia, da ogni attività eversiva e da ogni forma di aggressione criminale o terroristica.

2. Spettano all'AISI le attività di informazione per la sicurezza, che si svolgono all'interno del territorio nazionale, a protezione degli interessi politici, militari, economici, scientifici e industriali dell'Italia.

3. È, altresì, compito dell'AISI individuare e contrastare all'interno del territorio nazionale le attività di spionaggio dirette contro l'Italia e le attività volte a danneggiare gli interessi nazionali.

4. L'AISI può svolgere operazioni all'estero soltanto in collaborazione con l'AISE, quando tali operazioni siano strettamente connesse ad attività che la stessa AISI svolge all'interno del territorio nazionale. A tal fine il direttore generale del DIS provvede ad assicurare le necessarie forme di coordinamento e di raccordo informativo, anche al fine di evitare sovrapposizioni funzionali o territoriali.

5. L'AISI risponde al Presidente del Consiglio dei ministri.

6. L'AISI informa tempestivamente e con continuità il Ministro dell'interno, il Ministro degli affari esteri e il Ministro della difesa per i profili di rispettiva competenza.

7. Il Presidente del Consiglio dei ministri nomina e revoca, con proprio decreto, il direttore dell'AISI, scelto tra i dirigenti di prima fascia o equiparati dell'amministrazione dello Stato, sentito il CISR. L'incarico ha la durata massima di otto anni ed è conferibile, senza soluzione di continuità, anche con provvedimenti successivi, ciascuno dei quali di durata non superiore al quadriennio.

8. Il direttore dell'AISI riferisce costantemente sull'attività svolta al Presidente del Consiglio dei ministri o all'Autorità delegata, ove istituita, per il tramite del direttore generale del DIS. Riferisce direttamente al Presidente del Consiglio dei ministri in caso di urgenza o quando altre particolari circostanze lo richiedano, informandone senza ritardo il direttore generale del DIS; presenta al CISR, per il tramite del direttore generale del DIS, un rapporto annuale sul funzionamento e sull'organizzazione dell'Agenzia.

9. Il Presidente del Consiglio dei ministri nomina e revoca, sentito il direttore dell'AISI, uno o più vicedirettori. Il direttore dell'AISI affida gli altri incarichi nell'ambito dell'Agenzia.

10. L'organizzazione e il funzionamento dell'AISI sono disciplinati con apposito regolamento».

«Art. 43 (Procedura per l'adozione dei regolamenti). — 1. Salvo che non sia diversamente stabilito, le disposizioni regolamentari previste dalla presente legge sono emanate entro centottanta giorni dalla data della sua entrata in vigore, con uno o più decreti del Presidente del Consiglio dei ministri adottati anche in deroga all'articolo 17 della legge 23 agosto 1988, n. 400, e successive modificazioni, previo parere del Comitato parlamentare di cui all'articolo 30 e sentito il CISR.



2. I suddetti decreti stabiliscono il regime della loro pubblicità, anche in deroga alle norme vigenti.»

— Si riporta il testo degli articoli 1, 11 e 13 del decreto-legge 14 giugno 2021, n. 82, recante: «Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale», pubblicato nella *Gazzetta Ufficiale* n. 140 del 14 giugno 2021, convertito con modificazioni dalla legge 4 agosto 2021, n. 109:

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

a) cybersicurezza, l'insieme delle attività, fermi restando le attribuzioni di cui alla legge 3 agosto 2007, n. 124, e gli obblighi derivanti da trattati internazionali, necessarie per proteggere dalle minacce informatiche reti, sistemi informativi, servizi informatici e comunicazioni elettroniche, assicurandone la disponibilità, la confidenzialità e l'integrità e garantendone la resilienza, anche ai fini della tutela della sicurezza nazionale e dell'interesse nazionale nello spazio cibernetico;

b) resilienza nazionale nello spazio cibernetico, le attività volte a prevenire un pregiudizio per la sicurezza nazionale come definito dall'articolo 1, comma 1, lettera f), del regolamento di cui al decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131.

c) decreto-legge perimetro, 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;

d) decreto legislativo NIS, il decreto legislativo di recepimento della direttiva (UE) 2022/2555, del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148;

e) strategia nazionale di cybersicurezza, la strategia (di cui all'articolo 9) del decreto legislativo NIS.»

«Art. 11 (*Norme di contabilità e disposizioni finanziarie*). — 1. Con la legge di bilancio è determinato lo stanziamento annuale da assegnare all'Agenzia da iscriverne sul capitolo di cui all'articolo 18, comma 1, sulla base della determinazione del fabbisogno annuo operata dal Presidente del Consiglio dei ministri, previamente comunicata al COPASIR.

2. Le entrate dell'Agenzia sono costituite da:

a) dotazioni finanziarie e contributi ordinari di cui all'articolo 18 del presente decreto;

b) corrispettivi per i servizi prestati a soggetti pubblici o privati;

c) proventi derivanti dallo sfruttamento della proprietà industriale, dei prodotti dell'ingegno e delle invenzioni dell'Agenzia;

d) altri proventi patrimoniali e di gestione;

e) contributi dell'Unione europea o di organismi internazionali, anche a seguito della partecipazione a specifici bandi, progetti e programmi di collaborazione;

f) proventi delle sanzioni irrogate dall'Agenzia ai sensi di quanto previsto dal decreto legislativo NIS, dal decreto-legge perimetro e dal decreto legislativo 1° agosto 2003, n. 259, e relative disposizioni attuative;

g) ogni altra eventuale entrata.

3. Il regolamento di contabilità dell'Agenzia, che ne assicura l'autonomia gestionale e contabile, è adottato con decreto del Presidente del Consiglio dei ministri, di concerto con il Ministro dell'economia e delle finanze, su proposta del direttore generale dell'Agenzia, previo parere del COPASIR e sentito il CIC, entro centoventi giorni dalla data di entrata in vigore della legge di conversione del presente decreto, anche in deroga all'articolo 17 della legge 23 agosto 1988, n. 400, e alle norme di contabilità generale dello Stato e nel rispetto dei principi fondamentali da esse stabiliti, nonché delle seguenti disposizioni:

a) il bilancio preventivo e il bilancio consuntivo adottati dal direttore generale dell'Agenzia sono approvati con decreto del Presidente del Consiglio dei ministri, previo parere del CIC, e sono trasmessi alla Corte dei conti che esercita il controllo previsto dall'articolo 3, comma 4, della legge 14 gennaio 1994, n. 20;

b) il bilancio consuntivo e la relazione della Corte dei conti sono trasmessi alle Commissioni parlamentari competenti e al COPASIR.

4. Con regolamento adottato con decreto del Presidente del Consiglio dei ministri, su proposta del direttore generale dell'Agenzia, entro

centoventi giorni dalla data di entrata in vigore della legge di conversione del presente decreto, anche in deroga all'articolo 17 della legge 23 agosto 1988, n. 400, e alle norme in materia di contratti pubblici, previo parere del COPASIR e sentito il CIC, sono definite le procedure per la stipula di contratti di appalti di lavori e forniture di beni e servizi per le attività dell'Agenzia finalizzate alla tutela della sicurezza nazionale nello spazio cibernetico, ferma restando la disciplina dell'articolo 162 del codice dei contratti pubblici relativi a lavori, servizi e forniture, di cui al decreto legislativo 18 aprile 2016, n. 50.»

«Art. 13 (*Trattamento dei dati personali*). — 1. Il trattamento dei dati personali svolto per finalità di sicurezza nazionale in applicazione del presente decreto è effettuato ai sensi dell'articolo 58, commi 2 e 3, del decreto legislativo 30 giugno 2003, n. 196.»

— Si riporta il testo dell'articolo 9, comma 1, della legge 16 marzo 2006, n. 146 recante: «Ratifica ed esecuzione della Convenzione e dei Protocolli delle Nazioni Unite contro il crimine organizzato transnazionale, adottati dall'Assemblea generale il 15 novembre 2000 ed il 31 maggio 2001» pubblicato nella *Gazzetta Ufficiale* n. 85, del 11 aprile 2006.

«Art. 9 (*Operazioni sotto copertura*). — 1. Fermo quanto disposto dall'articolo 51 del Codice penale, non sono punibili:

a) gli ufficiali di polizia giudiziaria della Polizia di Stato, dell'Arma dei carabinieri e del Corpo della guardia di finanza, appartenenti alle strutture specializzate o alla Direzione investigativa antimafia, nei limiti delle proprie competenze, i quali, nel corso di specifiche operazioni di polizia e, comunque, al solo fine di acquisire elementi di prova in ordine ai delitti previsti dagli articoli 317, 318, 319, 319-bis, 319-ter, 319-quater, primo comma, 320, 321, 322, 322-bis, 346-bis, 353, 353-bis, 452-bis, 452-ter, 452-quater, 452-sexies, 452-quaterdecies, 453, 454, 455, 460, 461, 473, 474, 517-quater, 629, 630, 644, 648-bis e 648-ter, nonché nel libro secondo, titolo XII, capo III, sezione I, del codice penale, ai delitti concernenti armi, munizioni, esplosivi, ai delitti previsti dall'articolo 12, commi 1, 3, 3-bis e 3-ter, del testo unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulla condizione dello straniero, di cui al decreto legislativo 25 luglio 1998, n. 286, nonché in ordine ai delitti previsti dagli articoli 255-bis, 255-ter, 256, commi 1, secondo periodo, 1-bis, 3 e 3-bis, 256-bis e 259 del decreto legislativo 3 aprile 2006, n. 152, e ai delitti previsti dal testo unico delle leggi in materia di disciplina degli stupefacenti e sostanze psicotrope, prevenzione, cura e riabilitazione dei relativi stati di tossicodipendenza, di cui al decreto del Presidente della Repubblica 9 ottobre 1990, n. 309, e dall'articolo 3 della legge 20 febbraio 1958, n. 75, anche per interposta persona, danno rifugio o comunque prestano assistenza agli associati, acquistano, ricevono, sostituiscono od occultano denaro o altra utilità, armi, documenti, sostanze stupefacenti o psicotrope, beni ovvero cose che sono oggetto, prodotto, profitto, prezzo o mezzo per commettere il reato o ne accettano l'offerta o la promessa o altrimenti ostacolano l'individuazione della loro provenienza o ne consentono l'impiego ovvero corrispondono denaro o altra utilità in esecuzione di un accordo illecito già concluso da altri, promettono o danno denaro o altra utilità richiesti da un pubblico ufficiale o da un incaricato di un pubblico servizio o sollecitati come prezzo della mediazione illecita verso un pubblico ufficiale o un incaricato di un pubblico servizio o per remunerarlo o compiono attività prodromiche e strumentali;

b) gli ufficiali di polizia giudiziaria appartenenti agli organismi investigativi della Polizia di Stato e dell'Arma dei carabinieri specializzati nell'attività di contrasto al terrorismo e all'eversione e del Corpo della guardia di finanza competenti nelle attività di contrasto al finanziamento del terrorismo, i quali, nel corso di specifiche operazioni di polizia e, comunque, al solo fine di acquisire elementi di prova in ordine ai delitti commessi con finalità di terrorismo o di eversione, anche per interposta persona, compiono le attività di cui alla lettera a) ovvero si introducono all'interno di un sistema informatico o telematico, danneggiano, deteriorano, cancellano, alterano o comunque intervengono su un sistema informatico o telematico ovvero su informazioni, dati e programmi in esso contenuti, attivano identità, anche digitali, domini e spazi informatici comunque denominati, anche attraverso il trattamento di dati personali di terzi, ovvero assumono il controllo o comunque si avvalgono dell'altrui dominio e spazio informatico comunque denominato o compiono attività prodromiche o strumentali;

b-bis) gli ufficiali di polizia giudiziaria degli organismi specializzati nel settore dei beni culturali, nell'attività di contrasto dei delitti di cui agli articoli 518-sexies e 518-septies del codice penale, i quali nel corso di specifiche operazioni di polizia e, comunque, al solo fine di acquisire elementi di prova, anche per interposta persona, compiono le attività di cui alla lettera a);



b-ter) gli ufficiali di polizia giudiziaria dell'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, i quali, nel corso di specifiche operazioni di polizia finalizzate al contrasto dei reati informatici commessi ai danni delle infrastrutture critiche informatizzate individuate dalla normativa nazionale e internazionale e, comunque, al solo fine di acquisire elementi di prova, anche per interposta persona, compiono le attività di cui alla lettera a) ovvero si introducono all'interno di un sistema informatico o telematico, danneggiano, deteriorano, cancellano, alterano o comunque intervengono su un sistema informatico o telematico ovvero su informazioni, dati e programmi in esso contenuti, attivano identità, anche digitali, domini e spazi informatici comunque denominati, anche attraverso il trattamento di dati personali di terzi, ovvero assumono il controllo o comunque si avvalgono dell'altrui dominio e spazio informatico comunque denominato o compiono attività prodromiche o strumentali.

Omissis».

— Si riporta il testo dell'articolo 58 del citato decreto legislativo 30 giugno 2003, n. 196:

«Art. 58 (*Trattamenti di dati personali per fini di sicurezza nazionale o difesa*). — 1. Ai trattamenti di dati personali effettuati dagli organismi di cui agli articoli 4, 6 e 7 della legge 3 agosto 2007, n. 124, sulla base dell'articolo 26 della predetta legge o di altre disposizioni di legge o regolamento o previste da atti amministrativi generali, ovvero relativi a dati coperti da segreto di Stato ai sensi degli articoli 39 e seguenti della medesima legge, si applicano le disposizioni di cui all'articolo 160, comma 4, nonché, in quanto compatibili, le disposizioni di cui agli articoli 2, 3, 8, 15, 16, 18, 25, 37, 41, 42 e 43 del decreto legislativo 18 maggio 2018, n. 51.

2. Fermo restando quanto previsto dal comma 1, ai trattamenti effettuati da soggetti pubblici per finalità di difesa o di sicurezza dello Stato, in base a disposizioni di legge o di regolamento o previste da atti amministrativi generali, che prevedano specificamente il trattamento, si applicano le disposizioni di cui al comma 1 del presente articolo, nonché quelle di cui agli articoli 23 e 24 del decreto legislativo 18 maggio 2018, n. 51.

3. Con uno o più regolamenti sono individuate le modalità di applicazione delle disposizioni di cui ai commi 1 e 2, in riferimento alle tipologie di dati, di interessati, di operazioni di trattamento eseguibili e di persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile ai sensi dell'articolo 2-quaterdecies, anche in relazione all'aggiornamento e alla conservazione. I regolamenti, negli ambiti di cui al comma 1, sono adottati ai sensi dell'articolo 43 della legge 3 agosto 2007, n. 124, e, negli ambiti di cui al comma 2, sono adottati con decreto del Presidente del Consiglio dei ministri, ai sensi dell'articolo 17, comma 3, della legge 23 agosto 1988, n. 400, su proposta dei Ministri competenti.

4. Con uno o più regolamenti adottati con decreto del Presidente della Repubblica su proposta del Ministro della difesa, sono disciplinate le misure attuative del presente decreto in materia di esercizio delle funzioni di difesa e sicurezza nazionale da parte delle Forze armate».

Note all'art. 7:

— Si riporta il testo all'articolo 2 del decreto legislativo 3 maggio 2024, n.62 recante: «Definizione della condizione di disabilità, della valutazione di base, di accomodamento ragionevole, della valutazione multidimensionale per l'elaborazione e attuazione del progetto di vita individuale personalizzato e partecipato», pubblicato nella *Gazzetta Ufficiale* n. 111 del 14 maggio 2024:

«Art. 2 (*Definizioni*). — 1. Ai fini del presente decreto, si applicano le seguenti definizioni:

a) “condizione di disabilità”: una duratura compromissione fisica, mentale, intellettiva, del neurosviluppo o sensoriale che, in interazione con barriere di diversa natura, può ostacolare la piena ed effettiva partecipazione nei diversi contesti di vita su base di uguaglianza con gli altri;

b) “persona con disabilità”: persona definita dall'articolo 3, comma 1, della legge 5 febbraio 1992, n. 104, come modificato dal presente decreto;

c) “ICF”: Classificazione internazionale del funzionamento, della disabilità e della salute - International Classification of Functioning Disability and Health (ICF), adottata dall'Organizzazione mondiale della sanità conformemente agli articoli 21, lettera b), e 22 del Protocollo concernente la costituzione dell'Organizzazione mondiale della sanità,

stipulato a New York il 22 luglio 1946, reso esecutivo con decreto legislativo del Capo provvisorio dello Stato 4 marzo 1947, n. 1068;

d) “ICD”: Classificazione internazionale delle malattie - International Classification of Diseases (ICD), adottata dall'Organizzazione mondiale della sanità conformemente agli articoli 21, lettera b), e 22 del Protocollo concernente la costituzione dell'Organizzazione mondiale della sanità, stipulato a New York il 22 luglio 1946, reso esecutivo con decreto legislativo del Capo provvisorio dello Stato 4 marzo 1947, n. 1068;

e) “duratura compromissione”: compromissione derivante da qualsiasi perdita, limitazione o anomalia a carico di strutture o di funzioni corporee, come classificate dalla ICF, che persiste nel tempo o per la quale è possibile una regressione o attenuazione solo nel lungo periodo;

f) “profilo di funzionamento”: descrizione dello stato di salute di una persona attraverso la codificazione delle funzioni e strutture corporee, delle attività e della partecipazione secondo la ICF tenendo conto della ICD, quale variabile evolutiva correlata all'età, alla condizione di salute, ai fattori personali e ai determinanti di contesto, che può comprendere anche il profilo di funzionamento ai fini scolastici;

g) “WHODAS”: WHO Disability Assessment Schedule, questionario di valutazione basato sull'ICF che misura la salute e la condizione di disabilità;

h) “sostegni servizi, gli interventi, le prestazioni e i benefici individuati a conclusione dell'accertamento della condizione di disabilità e nel progetto di vita per migliorare le capacità della persona e la sua inclusione, nonché per contrastare la restrizione nella sua partecipazione sociale, graduati in “sostegno” e “sostegno intensivo”, in ragione della frequenza, della durata e della continuità del sostegno;

i) “piano di intervento”: documento di pianificazione e di coordinamento dei sostegni individuali relativi ad un'area di intervento;

l) “valutazione di base”: procedimento volto ad accertare, attraverso l'utilizzo delle classificazioni ICD e ICF e dei correlati strumenti tecnici operativi di valutazione, la condizione di disabilità ai fini dell'accesso al sostegno, lieve o medio, o al sostegno intensivo, elevato o molto elevato;

m) “valutazione multidimensionale”: procedimento volto a delineare con la persona con disabilità il suo profilo di funzionamento all'interno dei suoi contesti di vita, anche rispetto agli ostacoli e ai facilitatori in essi presenti, e a definire, anche in base ai suoi desideri e alle sue aspettative e preferenze, gli obiettivi a cui deve essere diretto il progetto di vita;

n) “progetto di vita”: progetto individuale, personalizzato e partecipato della persona con disabilità che, partendo dai suoi desideri e dalle sue aspettative e preferenze, è diretto ad individuare, in una visione esistenziale unitaria, i sostegni, formali e informali, per consentire alla persona stessa di migliorare la qualità della propria vita, di sviluppare tutte le sue potenzialità, di poter scegliere i contesti di vita e partecipare in condizioni di pari opportunità rispetto agli altri;

o) “domini della qualità di vita”: ambiti o dimensioni rilevanti nella vita di una persona con disabilità valutabili con appropriati indicatori;

p) “budget di progetto”: insieme delle risorse umane, professionali, tecnologiche, strumentali ed economiche, pubbliche e private, attivabili anche in seno alla comunità territoriale e al sistema dei supporti informali, da destinare al progetto di vita».

Note all'art. 8:

— Il decreto legislativo 16 ottobre 2003, n. 288, recante: «Riordino della disciplina degli Istituti di ricovero e cura a carattere scientifico, a norma dell'articolo 42, comma 1, della legge 16 gennaio 2003, n. 3», è pubblicato nella *Gazzetta Ufficiale* n. 250 del 27 ottobre 2003.

— Si riporta il testo degli articoli 32 e 33 della Costituzione:

«Art. 32. — La Repubblica tutela la salute come fondamentale diritto dell'individuo e interesse della collettività, e garantisce cure gratuite agli indigenti.

Nessuno può essere obbligato a un determinato trattamento sanitario se non per disposizione di legge. La legge non può in nessun caso violare i limiti imposti dal rispetto della persona umana.

Art. 33. — L'arte e la scienza sono libere e libero ne è l'insegnamento.

La Repubblica detta le norme generali sull'istruzione ed istituisce scuole statali per tutti gli ordini e gradi.



Enti e privati hanno il diritto di istituire scuole ed istituti di educazione, senza oneri per lo Stato.

La legge, nel fissare i diritti e gli obblighi delle scuole non statali che chiedono la parità, deve assicurare ad esse piena libertà e ai loro alunni un trattamento scolastico equipollente a quello degli alunni di scuole statali.

È prescritto un esame di Stato per l'ammissione ai vari ordini e gradi di scuole o per la conclusione di essi e per l'abilitazione all'esercizio professionale.

Le istituzioni di alta cultura, università ed accademie, hanno il diritto di darsi ordinamenti autonomi nei limiti stabiliti dalle leggi dello Stato.

La Repubblica riconosce il valore educativo, sociale e di promozione del benessere psicofisico dell'attività sportiva in tutte le sue forme.».

— Per i riferimenti al Regolamento (UE) 2016/679 del parlamento europeo e del consiglio del 27 aprile 2016 si vedano le note all'articolo 4.

— Si riporta il testo dell'articolo 2-sexies del citato decreto legislativo 30 giugno 2003, n.196, recante:

«Art. 2-sexies (*Trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante*). — 1. I trattamenti delle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, del Regolamento, necessari per motivi di interesse pubblico rilevante ai sensi del paragrafo 2, lettera g), del medesimo articolo, sono ammessi qualora siano previsti dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o di regolamento o da atti amministrativi generali che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

1-bis. I dati personali relativi alla salute, pseudonimizzati, sono trattati, anche mediante interconnessione, dal Ministero della salute, dall'Istituto superiore di sanità (ISS), dall'Agenzia nazionale per i servizi sanitari regionali (AGENAS), dall'Agenzia italiana del farmaco (AIFA), dall'Istituto nazionale per la promozione della salute delle popolazioni migranti e per il contrasto delle malattie della povertà (INMP), nonché, relativamente ai propri assistiti, dalle regioni e dalle province autonome, nel rispetto delle finalità istituzionali di ciascuno, secondo le modalità individuate con decreto del Ministro della salute, adottato ai sensi del comma 1 previo parere del Garante per la protezione dei dati personali.

1-ter. Il Ministero della salute disciplina, con uno o più decreti adottati ai sensi del comma 1, l'interconnessione a livello nazionale dei sistemi informativi su base individuale, pseudonimizzati, vi incluso il fascicolo sanitario elettronico (FSE), compresi quelli gestiti dai soggetti di cui al comma 1-bis o da altre pubbliche amministrazioni che a tal fine adeguano i propri sistemi informativi.

I decreti di cui al primo periodo adottati, previo parere del Garante per la protezione dei dati personali, nel rispetto del Regolamento, del presente codice, del codice dell'amministrazione digitale di cui al decreto legislativo 7 marzo 2005, n. 82, e delle linee guida emanate dall'Agenzia per l'Italia digitale in materia di interoperabilità, definiscono le caratteristiche e disciplinano un ambiente di trattamento sicuro all'interno del quale vengono messi a disposizione dati anonimi o pseudonimizzati, per le finalità istituzionali di ciascuno, secondo le modalità individuate al comma 1.

2. Fermo quanto previsto dal comma 1, si considera rilevante l'interesse pubblico relativo a trattamenti effettuati da soggetti che svolgono compiti di interesse pubblico o connessi all'esercizio di pubblici poteri nelle seguenti materie:

- a) accesso a documenti amministrativi e accesso civico;
- b) tenuta degli atti e dei registri dello stato civile, delle anagrafi della popolazione residente in Italia e dei cittadini italiani residenti all'estero, e delle liste elettorali, nonché rilascio di documenti di riconoscimento o di viaggio o cambiamento delle generalità;
- c) tenuta di registri pubblici relativi a beni immobili o mobili;
- d) tenuta dell'anagrafe nazionale degli abilitati alla guida e dell'archivio nazionale dei veicoli;
- e) cittadinanza, immigrazione, asilo, condizione dello straniero e del profugo, stato di rifugiato;
- f) elettorato attivo e passivo ed esercizio di altri diritti politici, protezione diplomatica e consolare, nonché documentazione delle attività istituzionali di organi pubblici, con particolare riguardo alla reda-

zione di verbali e resoconti dell'attività di assemblee rappresentative, commissioni e di altri organi collegiali o assembleari;

g) esercizio del mandato degli organi rappresentativi, ivi compresa la loro sospensione o il loro scioglimento, nonché l'accertamento delle cause di ineleggibilità, incompatibilità o di decadenza, ovvero di rimozione o sospensione da cariche pubbliche;

h) svolgimento delle funzioni di controllo, indirizzo politico, inchiesta parlamentare o sindacato ispettivo e l'accesso a documenti riconosciuti dalla legge e dai regolamenti degli organi interessati per esclusive finalità direttamente connesse all'espletamento di un mandato elettivo;

i) attività dei soggetti pubblici dirette all'applicazione, anche tramite i loro concessionari, delle disposizioni in materia tributaria e doganale, comprese quelle di prevenzione e contrasto all'evasione fiscale;

l) attività di controllo e ispettive;

m) concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti e abilitazioni;

n) conferimento di onorificenze e ricompense, riconoscimento della personalità giuridica di associazioni, fondazioni ed enti, anche di culto, accertamento dei requisiti di onorabilità e di professionalità per le nomine, per i profili di competenza del soggetto pubblico, ad uffici anche di culto e a cariche direttive di persone giuridiche, imprese e di istituzioni scolastiche non statali, nonché rilascio e revoca di autorizzazioni o abilitazioni, concessione di patrocini, patronati e premi di rappresentanza, adesione a comitati d'onore e ammissione a cerimonie ed incontri istituzionali;

o) rapporti tra i soggetti pubblici e gli enti del terzo settore;

p) obiezione di coscienza;

q) attività sanzionatorie e di tutela in sede amministrativa o giudiziaria;

r) rapporti istituzionali con enti di culto, confessioni religiose e comunità religiose;

s) attività socio-assistenziali a tutela dei minori e soggetti bisognosi, non autosufficienti e incapaci;

t) attività amministrative e certificatorie correlate a quelle di diagnosi, assistenza o terapia sanitaria o sociale, ivi incluse quelle correlate ai trapianti d'organo e di tessuti nonché alle trasfusioni di sangue umano;

u) compiti del servizio sanitario nazionale e dei soggetti operanti in ambito sanitario, nonché compiti di igiene e sicurezza sui luoghi di lavoro e sicurezza e salute della popolazione, protezione civile, salvaguardia della vita e incolumità fisica;

v) programmazione, gestione, controllo e valutazione dell'assistenza sanitaria, ivi incluse l'istituzione, la gestione, la pianificazione e il controllo dei rapporti tra l'amministrazione ed i soggetti accreditati o convenzionati con il servizio sanitario nazionale;

z) vigilanza sulle sperimentazioni, farmacovigilanza, autorizzazione all'immissione in commercio e all'importazione di medicinali e di altri prodotti di rilevanza sanitaria;

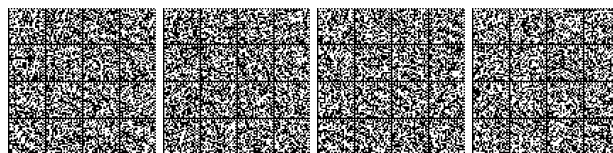
aa) tutela sociale della maternità ed interruzione volontaria della gravidanza, dipendenze, assistenza, integrazione sociale e diritti dei disabili;

bb) istruzione e formazione in ambito scolastico, professionale, superiore o universitario;

cc) trattamenti effettuati a fini di archiviazione nel pubblico interesse o di ricerca storica, concernenti la conservazione, l'ordinamento e la comunicazione dei documenti detenuti negli archivi di Stato negli archivi storici degli enti pubblici, o in archivi privati dichiarati di interesse storico particolarmente importante, per fini di ricerca scientifica, nonché per fini statistici da parte di soggetti che fanno parte del sistema statistico nazionale (Sistan);

dd) instaurazione, gestione ed estinzione, di rapporti di lavoro di qualunque tipo, anche non retribuito o onorario, e di altre forme di impiego, materia sindacale, occupazione e collocamento obbligatorio, previdenza e assistenza, tutela delle minoranze e pari opportunità nell'ambito dei rapporti di lavoro, adempimento degli obblighi retributivi, fiscali e contabili, igiene e sicurezza del lavoro o di sicurezza o salute della popolazione, accertamento della responsabilità civile, disciplinare e contabile, attività ispettiva.

3. Per i dati genetici, biometrici e relativi alla salute il trattamento avviene comunque nel rispetto di quanto previsto dall'articolo 2-septies.».



Note all'art. 9:

— Per i riferimenti al Regolamento (UE) 2016/679 del parlamento europeo e del consiglio del 27 aprile 2016 si vedano le note all'articolo 4.

Note all'art. 10:

— Il decreto-legge 18 ottobre 2012, n. 179 recante: «Ulteriori misure urgenti per la crescita del Paese» è pubblicato nella *Gazzetta Ufficiale* n. 245 del 19 ottobre 2012.

Note all'art. 11:

— Si riporta il testo dell'articolo 1-bis, del decreto legislativo 26 maggio 1997, n. 152 recante: «Attuazione della direttiva 91/533/CEE concernente l'obbligo del datore di lavoro di informare il lavoratore delle condizioni applicabili al contratto o al rapporto di lavoro», pubblicato nella *Gazzetta Ufficiale* n. 135 del 12 giugno 1997:

«Art. 1-bis (Ulteriori obblighi informativi nel caso di utilizzo di sistemi decisionali o di monitoraggio automatizzati). — 1. Il datore di lavoro o il committente pubblico e privato è tenuto a informare il lavoratore dell'utilizzo di sistemi decisionali o di monitoraggio integralmente automatizzati deputati a fornire indicazioni rilevanti ai fini della assunzione o del conferimento dell'incarico, della gestione o della cessazione del rapporto di lavoro, dell'assegnazione di compiti o mansioni nonché indicazioni incidenti sulla sorveglianza, la valutazione, le prestazioni e l'adempimento delle obbligazioni contrattuali dei lavoratori. Resta fermo quanto disposto dall'articolo 4 della legge 20 maggio 1970, n. 300.

2. Ai fini dell'adempimento degli obblighi di cui al comma 1, il datore di lavoro o il committente è tenuto a fornire al lavoratore, unitamente alle informazioni di cui all'articolo 1, prima dell'inizio dell'attività lavorativa, le seguenti ulteriori informazioni:

- a) gli aspetti del rapporto di lavoro sui quali incide l'utilizzo dei sistemi di cui al comma 1;
- b) gli scopi e le finalità dei sistemi di cui al comma 1;
- c) la logica ed il funzionamento dei sistemi di cui al comma 1;
- d) le categorie di dati e i parametri principali utilizzati per programmare o addestrare i sistemi di cui al comma 1, inclusi i meccanismi di valutazione delle prestazioni;
- e) le misure di controllo adottate per le decisioni automatizzate, gli eventuali processi di correzione e il responsabile del sistema di gestione della qualità;
- f) il livello di accuratezza, robustezza e cybersicurezza dei sistemi di cui al comma 1 e le metriche utilizzate per misurare tali parametri, nonché gli impatti potenzialmente discriminatori delle metriche stesse.

3. Il lavoratore, direttamente o per il tramite delle rappresentanze sindacali aziendali o territoriali, ha diritto di accedere ai dati e di richiedere ulteriori informazioni concernenti gli obblighi di cui al comma 2. Il datore di lavoro o il committente sono tenuti a trasmettere i dati richiesti e a rispondere per iscritto entro trenta giorni.

4. Il datore di lavoro o il committente sono tenuti a integrare l'informativa con le istruzioni per il lavoratore in merito alla sicurezza dei dati e l'aggiornamento del registro dei trattamenti riguardanti le attività di cui al comma 1, incluse le attività di sorveglianza e monitoraggio. Al fine di verificare che gli strumenti utilizzati per lo svolgimento della prestazione lavorativa siano conformi alle disposizioni previste dal Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, il datore di lavoro o il committente effettuano un'analisi dei rischi e una valutazione d'impatto degli stessi trattamenti, procedendo a consultazione preventiva del Garante per la protezione dei dati personali ove sussistano i presupposti di cui all'articolo 36 del Regolamento medesimo.

5. I lavoratori, almeno 24 ore prima, devono essere informati per iscritto di ogni modifica incidente sulle informazioni fornite ai sensi del comma 2 che comportino variazioni delle condizioni di svolgimento del lavoro.

6. Le informazioni e i dati di cui ai commi da 1 a 5 del presente articolo devono essere comunicati dal datore di lavoro o dal committente ai lavoratori in modo trasparente, in formato strutturato, di uso comune e leggibile da dispositivo automatico. La comunicazione delle medesime informazioni e dati deve essere effettuata anche alle rappresentanze sindacali aziendali ovvero alla rappresentanza sindacale unitaria e, in assenza delle predette rappresentanze, alle sedi territoriali delle associazioni sindacali comparativamente più rappresentative sul piano nazionale. Il Ministero del lavoro e delle politiche sociali e l'Ispettorato

nazionale del lavoro possono richiedere la comunicazione delle medesime informazioni e dati e l'accesso agli stessi.

7. Gli obblighi informativi di cui al presente articolo gravano anche sul committente nell'ambito dei rapporti di lavoro di cui all'articolo 409, n. 3, del codice di procedura civile e di cui all'articolo 2, comma 1, del decreto legislativo 15 giugno 2015, n. 81.

8. Gli obblighi informativi di cui al presente articolo non si applicano ai sistemi protetti da segreto industriale e commerciale.»

Note all'art. 15:

— Per i riferimenti al regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024, si vedano le note all'articolo 1.

— Si riporta il testo dell'articolo 12 decreto legislativo 30 gennaio 2006, n. 26, recante: «Attuazione della direttiva (UE) 2019/1024 relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico che ha abrogato la direttiva 2003/98/CE», pubblicato nella *Gazzetta Ufficiale* n. 28 del 3 febbraio 2006:

«Art. 12 (Funzioni). — 1. I componenti del comitato direttivo svolgono anche i compiti di responsabili di settore, curando, nell'ambito assegnato dallo stesso comitato direttivo:

- a) la predisposizione della bozza di programma annuale delle attività didattiche, da sottoporre al comitato direttivo, elaborata tenendo conto delle linee programmatiche sulla formazione pervenute dal Consiglio superiore della magistratura e dal Ministro della giustizia, nonché delle proposte pervenute dal Consiglio nazionale forense e dal Consiglio universitario nazionale;
- b) l'attuazione del programma annuale dell'attività didattica approvato dal comitato direttivo;
- c) la definizione del contenuto analitico di ciascuna sessione;
- d) l'individuazione dei docenti chiamati a svolgere l'incarico di insegnamento in ciascuna sessione, utilizzando lo specifico albo tenuto presso la Scuola, e la proposta dei relativi nominativi, in numero doppio rispetto agli incarichi, al comitato direttivo;
- e) la proposta dei criteri di ammissione alle sessioni di formazione;
- f) l'offerta di sussidio didattico e di sperimentazione di nuove formule didattiche;
- g) lo svolgimento delle sessioni presentando, all'esito di ciascuna di esse, relazioni consuntive;
- g-bis) l'individuazione di esperti formatori, scelti tra magistrati, docenti universitari e avvocati con adeguata qualificazione professionale ed esperienza organizzativa e formativa, nonché tra altri esperti qualificati, per i compiti previsti dal regolamento interno.»

Note all'art. 16:

— Per i riferimenti al regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024, si vedano le note all'articolo 1.

Note all'art. 17:

— Si riporta il testo dell'articolo 9 del codice di procedura civile, come modificato dalla presente legge:

«Art. 9 (Competenza del tribunale). — Il tribunale è competente per tutte le cause che non sono di competenza di altro giudice.

Il tribunale è altresì esclusivamente competente per le cause in materia di imposte e tasse, per quelle relative allo stato e alla capacità delle persone e ai diritti onorifici, per la querela di falso, per l'esecuzione forzata, per le cause che hanno ad oggetto il funzionamento di un sistema di intelligenza artificiale e, in generale, per ogni causa di valore indeterminabile.»

Note all'art. 18:

— Si riporta il testo dell'articolo 7, comma 1, del citato decreto-legge 14 giugno 2021, n. 82, come modificato dalla presente legge:

«Art. 7 (Funzioni dell'Agenzia per la cybersicurezza nazionale). — 1. L'Agenzia:

- a) è Autorità nazionale per la cybersicurezza e, in relazione a tale ruolo, assicura, nel rispetto delle competenze attribuite dalla normativa vigente ad altre amministrazioni, ferme restando le attribuzioni del Ministro dell'interno in qualità di autorità nazionale di pubblica si-



curezza, ai sensi della legge 1° aprile 1981, n. 121, il coordinamento tra i soggetti pubblici coinvolti in materia di cybersicurezza a livello nazionale e promuove la realizzazione di azioni comuni dirette ad assicurare la sicurezza e la resilienza cibernetiche per lo sviluppo della digitalizzazione del Paese, del sistema produttivo e delle pubbliche amministrazioni, nonché per il conseguimento dell'autonomia, nazionale ed europea, riguardo a prodotti e processi informatici di rilevanza strategica a tutela degli interessi nazionali nel settore. Per le reti, i sistemi informativi e i servizi informatici attinenti alla gestione delle informazioni classificate restano fermi sia quanto previsto dal regolamento adottato ai sensi dell'articolo 4, comma 3, lettera *l)*, della legge n. 124 del 2007, sia le competenze dell'Ufficio centrale per la segretezza di cui all'articolo 9 della medesima legge n. 124 del 2007;

b) predispone la strategia nazionale di cybersicurezza;

c) svolge ogni necessaria attività di supporto al funzionamento del Nucleo per la cybersicurezza, di cui all'articolo 8;

d) è Autorità nazionale competente NIS e Punto di contatto unico NIS di cui all'articolo 2, comma 1, lettere *d)* ed *e)*, del decreto legislativo NIS, a tutela dell'unità giuridica dell'ordinamento;

d-bis) è Autorità nazionale di gestione delle crisi informatiche di cui all'articolo 2, comma 1, lettera *g)*, del decreto legislativo NIS;

d-ter) è CSIRT nazionale, denominato CSIRT Italia, di cui all'articolo 2, comma 1, lettera *i)*, del decreto legislativo NIS;

e) è Autorità nazionale di certificazione della cybersicurezza ai sensi dell'articolo 58 del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, e assume tutte le funzioni in materia di certificazione di sicurezza cibernetica già attribuite al Ministero dello sviluppo economico dall'ordinamento vigente, comprese quelle relative all'accertamento delle violazioni e all'irrogazione delle sanzioni; nello svolgimento dei compiti di cui alla presente lettera:

1) accredita, ai sensi dell'articolo 60, paragrafo 1, del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, le strutture specializzate del Ministero della difesa e del Ministero dell'interno quali organismi di valutazione della conformità per i sistemi di rispettiva competenza;

2) delega, ai sensi dell'articolo 56, paragrafo 6, lettera *b)*, del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, il Ministero della difesa e il Ministero dell'interno, attraverso le rispettive strutture accreditate di cui al numero 1) della presente legge, al rilascio del certificato europeo di sicurezza cibernetica;

e-bis) è Autorità competente per l'esecuzione dei compiti previsti dal regolamento delegato (UE) 2024/1366 della Commissione, dell'11 marzo 2024, che integra il regolamento (UE) 2019/943 del Parlamento europeo e del Consiglio;

f) assume tutte le funzioni in materia di cybersicurezza già attribuite dalle disposizioni vigenti al Ministero dello sviluppo economico, ivi comprese quelle relative:

1) al perimetro di sicurezza nazionale cibernetica, di cui al decreto-legge perimetro e ai relativi provvedimenti attuativi, ivi incluse le funzioni attribuite al Centro di valutazione e certificazione nazionale ai sensi del decreto-legge perimetro, le attività di ispezione e verifica di cui all'articolo 1, comma 6, lettera *c)*, del decreto-legge perimetro e quelle relative all'accertamento delle violazioni e all'irrogazione delle sanzioni amministrative previste dal medesimo decreto, fatte salve quelle di cui all'articolo 3 del regolamento adottato con decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131;

2) alla sicurezza e all'integrità delle comunicazioni elettroniche, di cui agli articoli 16-*bis* e 16-*ter* del decreto legislativo 1° agosto 2003, n. 259, e relative disposizioni attuative;

3) alla sicurezza delle reti e dei sistemi informativi, di cui al decreto legislativo NIS;

g) partecipa, per gli ambiti di competenza, al gruppo di coordinamento istituito ai sensi dei regolamenti di cui all'articolo 1, comma 8, del decreto-legge 15 marzo 2012, n. 21, convertito, con modificazioni, dalla legge 11 maggio 2012, n. 56;

h) assume tutte le funzioni attribuite alla Presidenza del Consiglio dei ministri in materia di perimetro di sicurezza nazionale cibernetica, di cui al decreto-legge perimetro e ai relativi provvedimenti attuativi, ivi incluse le attività di ispezione e verifica di cui all'articolo 1, comma 6, lettera *c)*, del decreto-legge perimetro e quelle relative all'accertamento delle violazioni e all'irrogazione delle sanzioni amministrative previste dal medesimo decreto, fatte salve quelle di cui all'articolo 3 del regolamento adottato con decreto del Presidente del Consiglio dei ministri n. 131 del 2020;

i) assume tutte le funzioni già attribuite al Dipartimento delle informazioni per la sicurezza (DIS), di cui all'articolo 4 della legge 3 agosto 2007, n. 124, dal decreto-legge perimetro e dai relativi provvedimenti attuativi e supporta il Presidente del Consiglio dei ministri ai fini dell'articolo 1, comma 19-*bis*, del decreto-legge perimetro;

l) provvede, sulla base delle attività di competenza del Nucleo per la cybersicurezza di cui all'articolo 8, alle attività necessarie per l'attuazione e il controllo dell'esecuzione dei provvedimenti assunti dal Presidente del Consiglio dei ministri ai sensi dell'articolo 5 del decreto-legge perimetro;

m) assume tutte le funzioni in materia di cybersicurezza già attribuite all'Agenzia per l'Italia digitale dalle disposizioni vigenti e, in particolare, quelle di cui all'articolo 51 del decreto legislativo 7 marzo 2005, n. 82, nonché quelle in materia di adozione di linee guida contenenti regole tecniche di cybersicurezza ai sensi dell'articolo 71 del medesimo decreto legislativo. L'Agenzia assume, altresì, i compiti di cui all'articolo 33-*septies*, comma 4, del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, già attribuiti all'Agenzia per l'Italia digitale;

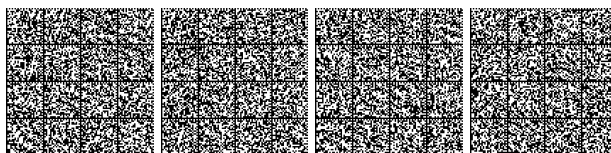
m-bis) provvede, anche attraverso un'apposita sezione nell'ambito della strategia di cui alla lettera *b)*, allo sviluppo e alla diffusione di standard, linee guida e raccomandazioni al fine di rafforzare la cybersicurezza dei sistemi informatici, alla valutazione della sicurezza dei sistemi crittografici nonché all'organizzazione e alla gestione di attività di divulgazione finalizzate a promuovere l'utilizzo della crittografia, anche a vantaggio della tecnologia blockchain, come strumento di cybersicurezza. L'Agenzia, anche per il rafforzamento dell'autonomia industriale e tecnologica dell'Italia, promuove altresì la collaborazione con centri universitari e di ricerca per la valorizzazione dello sviluppo di nuovi algoritmi proprietari, la ricerca e il conseguimento di nuove capacità crittografiche nazionali nonché la collaborazione internazionale con gli organismi esteri che svolgono analoghe funzioni. A tale fine, è istituito presso l'Agenzia, nell'ambito delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente e senza nuovi o maggiori oneri a carico della finanza pubblica, il Centro nazionale di crittografia, il cui funzionamento è disciplinato con provvedimento del direttore generale dell'Agenzia stessa. Il Centro nazionale di crittografia svolge le funzioni di centro di competenza nazionale per tutti gli aspetti della crittografia in ambito non classificato, ferme restando le competenze dell'Ufficio centrale per la segretezza, di cui all'articolo 9 della legge 3 agosto 2007, n. 124, con riferimento alle informazioni e alle attività previste dal regolamento adottato ai sensi dell'articolo 4, comma 3, lettera *l)*, della citata legge n. 124 del 2007, nonché le competenze degli organismi di cui agli articoli 4, 6 e 7 della medesima legge;

m-ter) provvede alla qualificazione dei servizi cloud per la pubblica amministrazione nel rispetto della disciplina dell'Unione europea e del regolamento di cui all'articolo 33-*septies*, comma 4, del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221;

m-quater) promuove e sviluppa ogni iniziativa, anche attraverso la conclusione di accordi di collaborazione con i privati, comunque denominati, nonché di partenariato pubblico-privato, volta a valorizzare l'intelligenza artificiale come risorsa per il rafforzamento della cybersicurezza nazionale;

n) sviluppa capacità nazionali di prevenzione, monitoraggio, rilevamento, analisi e risposta, per prevenire e gestire gli incidenti di sicurezza informatica e gli attacchi informatici, anche attraverso il CSIRT Italia di cui all'articolo 2, comma 1, lettera *i)* del decreto legislativo NIS. A tale fine, promuove iniziative di partenariato pubblico-privato per rendere effettive tali capacità;

n-bis) nell'ambito delle funzioni di cui al primo periodo della lettera *n)*, svolge ogni attività diretta all'analisi e al supporto per il contenimento e il ripristino dell'operatività dei sistemi compromessi, con la collaborazione dei soggetti pubblici o privati che hanno subito incidenti di sicurezza informatica o attacchi informatici. La mancata collaborazione di cui al primo periodo è valutata ai fini dell'applicazione delle sanzioni previste dall'articolo 1, commi 10 e 14, del decreto-legge perimetro, per i soggetti di cui all'articolo 1, comma 2-*bis*, del medesimo decreto-legge perimetro, i soggetti essenziali e i soggetti importanti di cui all'articolo 6 del decreto legislativo NIS, del decreto legislativo NIS e di cui all'articolo 40, comma 3, alinea, del codice delle comunicazioni elettroniche, di cui al decreto legislativo 1° agosto 2003, n. 259; restano esclusi gli organi dello Stato preposti alla prevenzione, all'accertamento e alla repressione dei reati, alla tutela dell'ordine e della sicurezza pub-



blica e alla difesa e sicurezza militare dello Stato, nonché gli organismi di informazione per la sicurezza di cui agli articoli 4, 6 e 7 della legge 3 agosto 2007, n. 124;

n-ter) provvede alla raccolta, all'elaborazione e alla classificazione dei dati relativi alle notifiche di incidenti ricevute dai soggetti che a ciò siano tenuti in osservanza delle disposizioni vigenti. Tali dati sono resi pubblici nell'ambito della relazione prevista dall'articolo 14, comma 1, quali dati ufficiali di riferimento degli attacchi informatici portati ai soggetti che operano nei settori rilevanti per gli interessi nazionali nel campo della cybersicurezza. Agli adempimenti previsti dalla presente lettera si provvede con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente;

o) partecipa alle esercitazioni nazionali e internazionali che riguardano la simulazione di eventi di natura cibernetica al fine di innalzare la resilienza del Paese;

p) cura e promuove la definizione ed il mantenimento di un quadro giuridico nazionale aggiornato e coerente nel dominio della cybersicurezza, tenendo anche conto degli orientamenti e degli sviluppi in ambito internazionale. A tal fine, l'Agenzia esprime pareri non vincolanti sulle iniziative legislative o regolamentari concernenti la cybersicurezza;

q) coordina, in raccordo con il Ministero degli affari esteri e della cooperazione internazionale, la cooperazione internazionale nella materia della cybersicurezza. Nell'ambito dell'Unione europea e a livello internazionale, l'Agenzia cura i rapporti con i competenti organismi, istituzioni ed enti, nonché segue nelle competenti sedi istituzionali le tematiche di cybersicurezza, fatta eccezione per gli ambiti in cui la legge attribuisce specifiche competenze ad altre amministrazioni. In tali casi, è comunque assicurato il raccordo con l'Agenzia al fine di garantire posizioni nazionali unitarie e coerenti con le politiche di cybersicurezza definite dal Presidente del Consiglio dei ministri;

r) perseguendo obiettivi di eccellenza, supporta negli ambiti di competenza, mediante il coinvolgimento del sistema dell'università e della ricerca nonché del sistema produttivo nazionali, lo sviluppo di competenze e capacità industriali, tecnologiche e scientifiche. A tali fini, l'Agenzia può promuovere, sviluppare e finanziare specifici progetti ed iniziative, volti anche a favorire il trasferimento tecnologico dei risultati della ricerca nel settore.

L'Agenzia assicura il necessario raccordo con le altre amministrazioni a cui la legge attribuisce competenze in materia di cybersicurezza e, in particolare, con il Ministero della difesa per gli aspetti inerenti alla ricerca militare. L'Agenzia può altresì promuovere la costituzione di aree dedicate allo sviluppo dell'innovazione finalizzate a favorire la formazione e il reclutamento di personale nei settori avanzati dello sviluppo della cybersicurezza, nonché promuovere la realizzazione di studi di fattibilità e di analisi valutative finalizzati a tale scopo;

s) stipula accordi bilaterali e multilaterali, anche mediante il coinvolgimento del settore privato e industriale, con istituzioni, enti e organismi di altri Paesi per la partecipazione dell'Italia a programmi di cybersicurezza, assicurando il necessario raccordo con le altre amministrazioni a cui la legge attribuisce competenze in materia di cybersicurezza, ferme restando le competenze del Ministero degli affari esteri e della cooperazione internazionale;

t) promuove, sostiene e coordina la partecipazione italiana a progetti e iniziative dell'Unione europea e internazionali, anche mediante il coinvolgimento di soggetti pubblici e privati nazionali, nel campo della cybersicurezza e dei correlati servizi applicativi, ferme restando le competenze del Ministero degli affari esteri e della cooperazione internazionale. L'Agenzia assicura il necessario raccordo con le altre amministrazioni a cui la legge attribuisce competenze in materia di cybersicurezza e, in particolare, con il Ministero della difesa per gli aspetti inerenti a progetti e iniziative in collaborazione con la NATO e con l'Agenzia europea per la difesa;

u) svolge attività di comunicazione e promozione della consapevolezza in materia di cybersicurezza, al fine di contribuire allo sviluppo di una cultura nazionale in materia;

v) promuove la formazione, la crescita tecnico-professionale e la qualificazione delle risorse umane nel campo della cybersicurezza, in particolare favorendo l'attivazione di percorsi formativi universitari in materia, anche attraverso l'assegnazione di borse di studio, di dottorato e assegni di ricerca, sulla base di apposite convenzioni con soggetti pubblici e privati; nello svolgimento di tali compiti, l'Agenzia può avvalersi anche delle strutture formative e delle capacità della Presidenza

del Consiglio dei ministri, del Ministero della difesa e del Ministero dell'interno, secondo termini e modalità da definire con apposito decreto del Presidente del Consiglio dei ministri, di concerto con i Ministri interessati;

v-bis) può predisporre attività di formazione specifica riservate ai giovani che aderiscono al servizio civile regolate sulla base di apposite convenzioni. In ogni caso, il servizio prestato è, a tutti gli effetti, riconosciuto come servizio civile;

z) per le finalità di cui al presente articolo, può costituire e partecipare a partenariati pubblico-privato sul territorio nazionale, nonché, previa autorizzazione del Presidente del Consiglio dei ministri, a consorzi, fondazioni o società con soggetti pubblici e privati, italiani e stranieri;

aa) è designata quale Centro nazionale di coordinamento ai sensi dell'articolo 6 del regolamento (UE) 2021/887 del Parlamento europeo e del Consiglio del 20 maggio 2021, che istituisce il Centro europeo di competenza per la cybersicurezza nell'ambito industriale, tecnologico e della ricerca e la rete dei centri nazionali di coordinamento.

Omissis.

Note all'art. 19:

— Si riporta il testo dell'articolo 8, commi da 1 a 3, del decreto-legge 1° marzo 2021, n. 22 recante: «Disposizioni urgenti in materia di riordino delle attribuzioni dei Ministeri», pubblicato nella *Gazzetta Ufficiale* n. 51 del 1° marzo 2021, convertito, con modificazioni, dalla legge 22 aprile 2021, n. 55, come modificato dalla presente legge:

«Art. 8 (*Funzioni in materia di innovazione tecnologica e transizione digitale e istituzione del Comitato interministeriale per la transizione digitale*). — 1. All'articolo 5, comma 3, della legge 23 agosto 1988, n. 400, dopo la lettera b), è aggiunta la seguente:

“b-bis) promuove, indirizza, coordina l'azione del Governo nelle materie dell'innovazione tecnologica, dell'attuazione dell'agenda digitale italiana ed europea, della strategia italiana per la banda ultralarga, della digitalizzazione delle pubbliche amministrazioni e delle imprese, nonché della trasformazione, crescita e transizione digitale del Paese, in ambito pubblico e privato, dell'accesso ai servizi in rete, della connettività, delle infrastrutture digitali materiali e immateriali e della strategia nazionale dei dati pubblici.”.

2. È istituito presso la Presidenza del Consiglio dei ministri il Comitato interministeriale per la transizione digitale (CITD), con il compito di assicurare, nelle materie di cui all'articolo 5, comma 3, lettera b-bis), della legge 23 agosto 1988, n. 400, come modificato dal presente decreto, il coordinamento e il monitoraggio dell'attuazione delle iniziative di innovazione tecnologica e transizione digitale delle pubbliche amministrazioni competenti in via ordinaria. Sono in ogni caso ricomprese prioritariamente nelle materie di competenza del Comitato, le attività di coordinamento e monitoraggio dell'attuazione delle iniziative relative:

a) alla strategia nazionale italiana per la banda ultralarga, alle reti di comunicazione elettronica satellitari, terrestri mobili e fisse;

b) al fascicolo sanitario elettronico e alla piattaforma dati sanitari;

c) allo sviluppo e alla diffusione delle tecnologie emergenti dell'intelligenza artificiale, dell'internet delle cose (IoT) e della blockchain.

3. Il Comitato è presieduto dal Presidente del Consiglio dei ministri o dalla Autorità delegata per l'innovazione tecnologica e la transizione digitale, ove nominata, ed è composto dai Ministri per la pubblica amministrazione, ove nominato, dell'economia e delle finanze, della giustizia, delle imprese e del made in Italy, dell'università e della ricerca e della salute, nonché dall'Autorità delegata per la sicurezza della Repubblica e per la cybersicurezza, ove nominata. Ad esso partecipano altresì gli altri Ministri o loro delegati aventi competenza nelle materie oggetto dei provvedimenti e delle tematiche poste all'ordine del giorno.

Omissis.

Note all'art. 20:

— Per i riferimenti al regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024, si vedano le note all'articolo 1.

— Per il testo dell'articolo 1 del citato decreto-legge 14 giugno 2021, n. 82, si vedano le note all'articolo 6.

— Si riporta il testo dell'articolo 36 del decreto-legge 30 aprile 2019, n. 34, recante: «Misure urgenti di crescita economica e per la



risoluzione di specifiche situazioni di crisi», pubblicato nella *Gazzetta Ufficiale* n. 100 del 30 aprile 2019, convertito, con modificazioni, dalla legge 28 giugno 2019, n. 58:

«Art. 36 (*Banche popolari e Fondo indennizzo risparmiatori*). —

1. All'articolo 1, comma 2, del decreto-legge 24 gennaio 2015, n. 3, convertito, con modificazioni, dalla legge 24 marzo 2015, n. 33, la parola: «2019» è sostituita dalla seguente: «2020».

2. All'articolo 1 della legge 30 dicembre 2018, n. 145, sono apportate le seguenti modifiche:

a) al comma 494, le parole «e aventi causa» sono sostituite dalle seguenti: «mortis causa, o il coniuge, il soggetto legato da unione civile, il convivente more uxorio o di fatto di cui alla legge 20 maggio 2016, n. 76, i parenti entro il secondo grado, ove siano succeduti nel possesso dei predetti strumenti finanziari in forza di trasferimento a titolo particolare per atto tra vivi»;

b) al comma 496, primo periodo, dopo le parole «costo di acquisto», sono inserite le seguenti: «inclusi gli oneri fiscali»;

c) al comma 497, primo periodo, dopo le parole «costo di acquisto», sono inserite le seguenti: «inclusi gli oneri fiscali»;

d) al comma 500, secondo periodo, dopo le parole «titoli di Stato con scadenza equivalente» sono aggiunte le seguenti: «determinato ai sensi dei commi 3, 4 e 5 dell'articolo 9 del decreto-legge 3 maggio 2016, n. 59, convertito, con modificazioni, dalla legge 30 giugno 2016, n. 119»;

e) al comma 501, i periodi secondo, terzo, quarto, quinto e sesto sono sostituiti dai seguenti:

«Con decreto del Ministro dell'economia e delle finanze sono definite le modalità di presentazione della domanda di indennizzo nonché i piani di riparto delle risorse disponibili. Con il medesimo decreto è istituita e disciplinata una Commissione tecnica per: l'esame delle domande e l'ammissione all'indennizzo del FIR; la verifica delle violazioni massive, nonché della sussistenza del nesso di causalità tra le medesime e il danno subito dai risparmiatori; l'erogazione dell'indennizzo da parte del FIR. Le suddette verifiche possono avvenire anche attraverso la preventiva tipizzazione delle violazioni massive e la corrispondente identificazione degli elementi oggettivi e/o soggettivi in presenza dei quali l'indennizzo può essere direttamente erogato. Il decreto indica i tempi delle procedure di definizione delle istanze presentate entro il termine di cui al penultimo periodo e, in modo non tassativo, le fattispecie di violazioni massive. Il suddetto procedimento non si applica ai casi di cui al comma 502-bis. La citata Commissione è composta da nove membri in possesso di idonei requisiti di competenza, indipendenza, onorabilità e probità. Con successivo decreto del Ministro dell'economia e delle finanze sono nominati i componenti della Commissione tecnica e determinati gli emolumenti da attribuire ai medesimi, nel limite massimo di 1,2 milioni di euro per ciascuno degli anni 2019, 2020 e 2021. Ai relativi oneri si provvede mediante la corrispondente riduzione della dotazione del FIR. Qualora l'importo dei compensi da attribuire ai componenti della Commissione tecnica risulti inferiore al predetto limite massimo, con decreto del Ministro dell'economia e delle finanze, l'importo eccedente confluisce nel FIR. Il Ministro dell'economia e delle finanze è autorizzato ad apportare le occorrenti variazioni di bilancio. La domanda di indennizzo, corredata di idonea documentazione attestante i requisiti di cui al comma 494, è inviata entro il termine di centottanta giorni decorrenti dalla data individuata con apposito decreto del Ministro dell'economia e delle finanze»;

f) dopo il comma 501 è inserito il seguente comma:

«501-bis. Le attività di supporto per l'espletamento delle funzioni della Commissione tecnica di cui al comma 501 sono affidate dal Ministro dell'economia e delle finanze, nel rispetto dei pertinenti principi dell'ordinamento nazionale e di quello dell'Unione europea, a società a capitale interamente pubblico, su cui l'amministrazione dello Stato esercita un controllo analogo a quello esercitato su propri servizi e che svolge la propria attività quasi esclusivamente nei confronti della predetta amministrazione.

Gli oneri e le spese relative alle predette attività sono a carico delle risorse finanziarie del FIR non oltre il limite massimo complessivo di 12,5 milioni di euro»;

g) il comma 502 è sostituito dal seguente:

«502. I risparmiatori di cui al comma 502-bis sono soddisfatti con priorità a valere sulla dotazione del FIR»;

h) dopo il comma 502, sono aggiunti i seguenti:

«502-bis. Previo accertamento da parte della Commissione tecnica di cui al comma 501 esclusivamente dei requisiti soggettivi e

oggettivi previsti nel presente comma, hanno diritto all'erogazione da parte del FIR di un indennizzo forfettario dell'ammontare determinato ai sensi dei precedenti commi 496 e 497 i risparmiatori persone fisiche, imprenditori individuali, anche agricoltori, coltivatori diretti, in possesso delle azioni e delle obbligazioni subordinate delle banche di cui al comma 493 alla data del provvedimento di messa in liquidazione coatta amministrativa - ovvero i loro successori mortis causa o il coniuge, il soggetto legato da unione civile, il convivente more uxorio o di fatto, i parenti entro il secondo grado in possesso dei suddetti strumenti finanziari a seguito di trasferimento con atto tra vivi - che soddisfano una delle seguenti condizioni: a) patrimonio mobiliare di proprietà del risparmiatore di valore inferiore a 100.000 euro; b) ammontare del reddito complessivo del risparmiatore ai fini dell'imposta sul reddito delle persone fisiche inferiore a 35.000 euro nell'anno 2018, al netto di eventuali prestazioni di previdenza complementare erogate sotto forma di rendita. Il valore del patrimonio mobiliare di cui alla suddetta lettera a) risulta dal patrimonio mobiliare posseduto al 31 dicembre 2018, esclusi gli strumenti finanziari di cui al comma 494, nonché i contratti di assicurazione a capitalizzazione o mista sulla vita, calcolato secondo i criteri e le istruzioni approvati con decreto del Ministero del lavoro e delle politiche sociali, Direzione generale per l'inclusione e le politiche sociali, di concerto con il Ministero dell'economia e delle finanze, Dipartimento delle finanze del 13 aprile 2017, n. 138, recante approvazione del modello tipo di dichiarazione sostitutiva unica (DSU), nonché delle relative istruzioni per la compilazione, ai sensi dell'articolo 10, comma 3, del decreto del Presidente del Consiglio dei ministri del 5 dicembre 2013, n. 159. Con il decreto del Ministro dell'economia e delle finanze previsto dal precedente comma 501 sono stabilite le modalità di presentazione dell'istanza di erogazione del menzionato indennizzo forfettario. Nell'erogazione degli indennizzi effettuata ai sensi del presente comma è data precedenza ai pagamenti di importo non superiore a 50.000 euro.

502-ter. Il limite di valore del patrimonio mobiliare di proprietà del risparmiatore, di cui al comma 502-bis, lettera a), può essere elevato fino a 200.000 euro con decreto del Presidente del Consiglio dei ministri, su proposta del Ministro dell'economia e delle finanze, previo assenso della Commissione europea. Il decreto del Ministro dell'economia e delle finanze di cui al comma 501, secondo periodo, è conseguentemente adeguato».

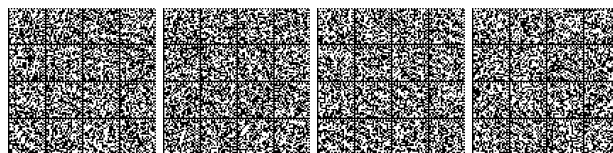
2-bis. Al fine di promuovere e sostenere l'imprenditoria, di stimolare la competizione nel mercato e di assicurare la protezione adeguata dei consumatori, degli investitori e del mercato dei capitali, nonché di favorire il raccordo tra le istituzioni, le autorità e gli operatori del settore, il Ministro dell'economia e delle finanze, sentiti la Banca d'Italia, la Commissione nazionale per le società e la borsa (CONSOB) e l'Istituto per la vigilanza sulle assicurazioni (IVASS), adotta, entro il 31 gennaio 2021, uno o più regolamenti per definire le condizioni e le modalità di svolgimento di una sperimentazione relativa alle attività di tecnologia (Fin.Tech) volte al perseguimento, mediante nuove tecnologie quali l'intelligenza artificiale e i registri distribuiti, dell'innovazione di servizi e di prodotti nei settori finanziario, creditizio, assicurativo e dei mercati regolamentati.

2-ter. La sperimentazione di cui al comma 2-bis si conforma al principio di proporzionalità previsto dalla normativa dell'Unione europea ed è caratterizzata da:

- a) una durata massima di diciotto mesi prorogabili per un massimo di ulteriori dodici mesi;
- b) requisiti patrimoniali ridotti;
- c) adempimenti semplificati e proporzionati alle attività che si intende svolgere;
- d) tempi ridotti delle procedure autorizzative;
- e) definizione di perimetri e limiti di operatività.

2-quater. Nel rispetto della normativa inderogabile dell'Unione europea, i regolamenti di cui al comma 2-bis stabiliscono o individuano i criteri per determinare:

- a) i requisiti di ammissione alla sperimentazione;
- a-bis) i casi in cui un'attività può essere ammessa a sperimentazione;
- a-ter) i casi in cui è ammessa la proroga;
- b) i requisiti patrimoniali;
- c) gli adempimenti semplificati e proporzionati alle attività che si intende svolgere;
- d) i perimetri di operatività;
- e) gli obblighi informativi;



- f) i tempi per il rilascio di autorizzazioni;
- g) i requisiti di professionalità degli esponenti aziendali;
- h) i profili di governo societario e di gestione del rischio;

i) le forme societarie ammissibili anche in deroga alle forme societarie previste dal testo unico delle leggi in materia bancaria e creditizia, di cui al decreto legislativo 1° settembre 1993, n. 385, dal testo unico delle disposizioni in materia di intermediazione finanziaria, di cui al decreto legislativo 24 febbraio 1998, n. 58, e dal codice delle assicurazioni private, di cui al decreto legislativo 7 settembre 2005, n. 209;

- l) le eventuali garanzie finanziarie;

m) l'iter successivo al termine della sperimentazione.

2-quinquies. Le misure di cui ai commi 2-ter e 2-quater possono essere differenziate e adeguate in considerazione delle particolarità e delle esigenze dei casi specifici; esse hanno carattere temporaneo e garantiscono adeguate forme di informazione e di protezione a favore di consumatori e investitori, nonché del corretto funzionamento dei mercati. L'operatività delle misure cessa al termine del relativo periodo, ovvero alla perdita dei requisiti o al superamento dei limiti operativi stabiliti, nonché negli altri casi previsti dai regolamenti di cui al comma 2-bis.

2-sexies. La sperimentazione non comporta il rilascio di autorizzazioni per l'esercizio di attività riservate da svolgersi al di fuori di essa. Lo svolgimento, nell'ambito della sperimentazione e nel rispetto dei limiti stabiliti dai provvedimenti di ammissione, di attività che rientrano nella nozione di servizi e attività di investimento non implica l'esercizio a titolo abituale di attività riservate e, pertanto, non necessita del rilascio di autorizzazioni ove sia prevista una durata massima di sei mesi, salvo il maggior termine della sperimentazione, che non può superare complessivamente il limite massimo di diciotto mesi, nei casi in cui sia concessa una proroga funzionale all'ottenimento dell'autorizzazione o dell'iscrizione prevista dalla legge per lo svolgimento abituale e a titolo professionale dell'attività medesima. Nel rispetto delle norme stabilite dai regolamenti di cui al comma 2-bis e delle finalità del periodo di sperimentazione, la Banca d'Italia, la CONSOB e l'IVASS, nell'ambito delle proprie competenze e delle materie seguite, adottano i provvedimenti per l'ammissione alla sperimentazione delle attività di cui al comma 2-bis e ogni altra iniziativa ad essi propedeutica. I provvedimenti per l'ammissione alla sperimentazione stabiliscono i limiti dell'attività di partecipazione alla sperimentazione con riguardo alla tipologia e alle modalità di prestazione del servizio di investimento, alla tipologia e al numero di utenti finali, al numero di operazioni, ai volumi complessivi dell'attività. Nel rispetto della normativa inderogabile dell'Unione europea, l'ammissione alla sperimentazione può comportare la deroga o la disapplicazione temporanea degli orientamenti di vigilanza o degli atti di carattere generale emanati dalle autorità di vigilanza, nonché delle norme o dei regolamenti emanati dalle medesime autorità di vigilanza, concernenti i profili di cui al comma 2-quater, lettere b), c), d), e), f), g), h), i) e l). Alle attività della Banca d'Italia, della CONSOB e dell'IVASS relative alla sperimentazione si applicano gli articoli 7 del testo unico di cui al decreto legislativo 1° settembre 1993, n. 385, 4 del testo unico di cui al decreto legislativo 24 febbraio 1998, n. 58, e 10 del codice di cui al decreto legislativo 7 settembre 2005, n. 209, nonché gli articoli 21 e 24, comma 6-bis, della legge 28 dicembre 2005, n. 262.

2-septies. La Banca d'Italia, la CONSOB e l'IVASS redigono annualmente, ciascuno per quanto di propria competenza, una relazione d'analisi sul settore tecno-finanziario, riportando quanto emerge dall'applicazione del regime di sperimentazione di cui al comma 2-bis, e segnalano eventuali modifiche normative o regolamentari necessarie per lo sviluppo del settore, la tutela del risparmio e la stabilità finanziaria.

2-octies. È istituito presso il Ministero dell'economia e delle finanze il Comitato FinTech. Il Comitato ha il compito di individuare gli obiettivi, definire i programmi e porre in essere le azioni per favorire lo sviluppo della tecno-finanza, anche in cooperazione con soggetti esteri, nonché di formulare proposte di carattere normativo e agevolare il contatto degli operatori del settore con le istituzioni e con le autorità. Sono membri permanenti del Comitato il Ministro dell'economia e delle finanze, il Ministro dello sviluppo economico, il Ministro per gli affari europei, la Banca d'Italia, la CONSOB, l'IVASS, l'Autorità garante della concorrenza e del mercato, il Garante per la protezione dei dati personali, l'Agenzia per l'Italia digitale e l'Agenzia delle entrate. Il Comitato può invitare alle proprie riunioni, con funzioni consultive e senza diritto di voto, ulteriori istituzioni e autorità, nonché associazioni di categoria, imprese, enti e soggetti operanti nel settore della tecno-finanza. I regolamenti di cui al comma 2-bis stabiliscono le attribuzioni del Comitato. Per le attività svolte dal Comitato relative alla sperimentazione, i membri permanenti collaborano tra loro, anche mediante scambio di in-

formazioni, e non possono reciprocamente opporsi il segreto d'ufficio. Dall'attuazione delle disposizioni dei commi da 2-bis al presente comma non devono derivare nuovi o maggiori oneri per la finanza pubblica.

2-novies. Le autorità di vigilanza e di controllo sono autorizzate, singolarmente o in collaborazione tra loro, a stipulare accordi con una o più università sottoposte alla vigilanza del Ministro dell'istruzione, dell'università e della ricerca e con centri di ricerca ad esse collegati, aventi ad oggetto lo studio dell'applicazione alla loro attività istituzionale degli strumenti di intelligenza artificiale, di registri contabili criptati e di registri distribuiti, nonché la formazione del proprio personale.

Agli oneri derivanti dagli accordi di cui al presente comma le autorità provvedono nell'ambito dei rispettivi stanziamenti di bilancio.

2-decies. All'articolo 24-bis del decreto-legge 23 dicembre 2016, n. 237, convertito, con modificazioni, dalla legge 17 febbraio 2017, n. 15, sono apportate le seguenti modificazioni:

- a) il comma 7 è sostituito dal seguente:

“7. Dall'istituzione del Comitato di cui al comma 6 non devono derivare oneri a carico della finanza pubblica, salvo quanto previsto dal comma 9”;

- b) il comma 9 è sostituito dal seguente:

“9. Il Comitato opera attraverso riunioni periodiche, prevedendo, ove necessario, la costituzione di specifici gruppi di ricerca cui possono partecipare accademici ed esperti nella materia.

La partecipazione al Comitato non dà titolo ad alcun emolumento o compenso o gettone di presenza. È fatta salva la corresponsione ai componenti del Comitato dei rimborsi delle spese di viaggio e di alloggio, sostenute per la partecipazione alle riunioni periodiche di cui al primo periodo, a valere sui fondi previsti dal comma 11”.

2-undecies. All'articolo 48-bis, comma 1, secondo periodo, del decreto del Presidente della Repubblica 29 settembre 1973, n. 602, sono aggiunte, in fine, le seguenti parole: “nonché ai risparmiatori di cui all'articolo 1, comma 494, della legge 30 dicembre 2018, n. 145, che hanno subito un pregiudizio ingiusto da parte di banche e loro controllate aventi sede legale in Italia, poste in liquidazione coatta amministrativa dopo il 16 novembre 2015 e prima del 16 gennaio 2018”.

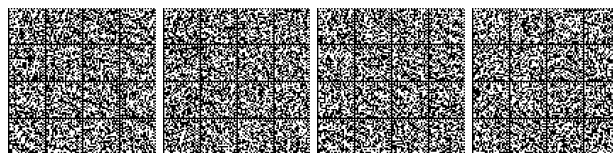
2-duodecies. All'articolo 5, comma 1, del decreto-legge 25 marzo 2019, n. 22, convertito, con modificazioni, dalla legge 20 maggio 2019, n. 41, le parole: “ad operarvi nel periodo transitorio,” sono sostituite dalle seguenti: “ad operare con le medesime modalità nel periodo transitorio,”.

2-terdecies. La CONSOB ordina ai fornitori di connettività alla rete internet ovvero ai gestori di altre reti telematiche o di telecomunicazione, o agli operatori che in relazione ad esse forniscono servizi telematici o di telecomunicazione, la rimozione delle iniziative di chiunque nel territorio della Repubblica, attraverso le reti telematiche o di telecomunicazione, offre o svolge servizi o attività di investimento senza esservi abilitato. I destinatari degli ordini comunicati ai sensi del primo periodo hanno l'obbligo di inibire l'utilizzazione delle reti delle quali sono gestori o in relazione alle quali forniscono servizi. La CONSOB può stabilire con regolamento le modalità e i termini degli adempimenti previsti dal presente comma.

2-quaterdecies. La Consob può ordinare ai soggetti di cui al comma 2-terdecies la rimozione delle campagne pubblicitarie condotte attraverso le reti telematiche o di telecomunicazione, aventi ad oggetto servizi o attività di investimento prestati da chi non vi è abilitato.”.

— Si riporta il testo dell'articolo 15 del decreto-legge 15 settembre 2023, n. 123, recante: «Misure urgenti di contrasto al disagio giovanile, alla povertà educativa e alla criminalità minorile, nonché per la sicurezza dei minori in ambito digitale», pubblicato nella *Gazzetta Ufficiale* n. 216 del 15 settembre 2023, convertito, con modificazioni, dalla legge 13 novembre 2023, n. 159:

«Art. 15 (*Designazione del coordinatore dei servizi digitali in attuazione del Regolamento (UE) 2022/2065 sui servizi digitali*). — 1. Al fine di garantire l'effettività dei diritti e l'efficacia degli obblighi stabiliti dal Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali, nonché la relativa vigilanza e il conseguimento degli obiettivi previsti, anche con riguardo alla protezione dei minori in relazione ai contenuti pornografici disponibili on line, nonché agli altri contenuti illegali o comunque vietati, veicolati da piattaforme on line o altri gestori di servizi intermediari, e contribuire alla definizione di un ambiente digitale sicuro, l'Autorità per le garanzie nelle comunicazioni è desi-



gnata quale Coordinatore dei Servizi Digitali, ai sensi dell'articolo 49, paragrafo 2, del Regolamento (UE) 2022/2065.

2. L'Autorità garante della concorrenza e del mercato, il Garante per la protezione dei dati personali e ogni altra Autorità nazionale competente, nell'ambito delle rispettive competenze, assicurano ogni necessaria collaborazione ai fini dell'esercizio da parte dell'Autorità per le garanzie nelle comunicazioni delle funzioni di Coordinatore dei Servizi Digitali. Le Autorità possono disciplinare con protocolli di intesa gli aspetti applicativi e procedurali della reciproca collaborazione.

3. L'Autorità per le garanzie nelle comunicazioni definisce, con proprio provvedimento, le condizioni, le procedure e le modalità operative per l'esercizio dei poteri e delle funzioni di cui è titolare, quale Coordinatore dei Servizi Digitali, ai sensi del Regolamento (UE) 2022/2065 e svolge i relativi compiti in modo imparziale, trasparente e tempestivo.

4. All'articolo 1 della legge 31 luglio 1997, n. 249, sono apportate le seguenti modificazioni:

a) al comma 6, lettera c), dopo il numero 14-bis) è aggiunto il seguente: «(14-ter) esercita la funzione di Coordinatore dei Servizi Digitali e i relativi poteri previsti dal Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali.»;

b) dopo il comma 32, è aggiunto il seguente:

«32-bis. In caso di violazione degli obblighi previsti agli articoli 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 20, 21, 22, 23, 24, 26, 27, 28, 30 e 45 del Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali, l'Autorità, nell'esercizio dei poteri di cui al combinato disposto degli articoli 51 e 52 del medesimo Regolamento (UE) 2022/2065, applica, in base a principi di proporzionalità, adeguatezza e rispetto del contraddittorio, secondo le procedure stabilite con proprio regolamento, sanzioni amministrative pecuniarie fino ad un massimo del 6% del fatturato annuo mondiale nell'esercizio finanziario precedente alla comunicazione di avvio del procedimento al prestatore di un servizio intermediario rientrante nella propria sfera di competenza, anche nella sua qualità di Coordinatore dei Servizi Digitali, ai sensi del diritto nazionale e dell'Unione europea applicabile alla fattispecie di illecito. In caso di comunicazione di informazioni inesatte, incomplete o fuorvianti, di mancata risposta o rettifica di informazioni inesatte, incomplete o fuorvianti e di inosservanza dell'obbligo di sottoporsi a un'ispezione, l'Autorità, nell'esercizio dei poteri di cui al combinato disposto degli articoli 51 e 52 del medesimo Regolamento (UE) 2022/2065, applica una sanzione amministrativa pecuniaria fino ad un massimo dell'1% del fatturato mondiale realizzato nell'esercizio finanziario precedente dal fornitore di un servizio intermediario o dalla persona interessata rientrante nella propria sfera di competenza, anche nella sua qualità di Coordinatore dei Servizi Digitali, ai sensi del diritto nazionale e dell'Unione europea applicabile alla fattispecie di illecito. L'importo massimo giornaliero delle penalità di mora che l'Autorità può applicare è pari al 5% del fatturato giornaliero medio mondiale del fornitore di un servizio intermediario interessato realizzato nell'esercizio finanziario precedente, calcolato a decorrere dalla data specificata nella decisione in questione. Nell'applicazione della sanzione l'Autorità tiene conto, in particolare, della gravità del fatto e delle conseguenze che ne sono derivate, nonché della durata e dell'eventuale reiterazione delle violazioni. Per le sanzioni amministrative previste dal presente comma è escluso il beneficio del pagamento in misura ridotta previsto dall'articolo 16 della legge 24 novembre 1981, n. 689.».

5. La pianta organica dell'Autorità per le garanzie nelle comunicazioni è incrementata in misura di 23 unità con le seguenti qualifiche: n. 1 dirigente, n. 20 funzionari, n. 2 operativi. Gli oneri derivanti dal presente articolo sono determinati in 4.005.457 euro per l'anno 2024, 4.125.590 euro per l'anno 2025, 3.903.136 euro per l'anno 2026, 4.081.636 euro per l'anno 2027, 4.267.375 euro per l'anno 2028, 4.527.751 euro per l'anno 2029, 4.737.357 euro per l'anno 2030, 4.971.989 euro per l'anno 2031, 5.434.808 euro per l'anno 2032 e 5.694.052 euro a decorrere dall'anno 2033. Ad essi si provvede mediante un contributo di importo pari allo 0,135 per mille del fatturato risultante dall'ultimo bilancio approvato dai prestatori dei servizi intermediari stabiliti in Italia, così come definiti dal Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la Direttiva 2000/31/CE (Regolamento sui servizi digitali). Ferme restando tutte le attuali forme di finanziamento e nel rispetto delle esenzioni previste dal Regolamento medesimo, in sede di prima applicazione, per l'anno 2024, il contributo è versato direttamente all'Autorità entro il 1° marzo 2024 nella misura dello 0,135

per mille del fatturato realizzato nell'anno contabile 2022 secondo le modalità determinate dall'Autorità medesima con propria deliberazione. Eventuali variazioni della misura e delle modalità di contribuzione, per gli anni successivi, possono essere motivatamente adottate dall'Autorità, con propria deliberazione, nel limite massimo dello 0,5 per mille del fatturato risultante dall'ultimo bilancio approvato. L'Autorità individua, con la collaborazione dell'Istituto nazionale di statistica (ISTAT) e dell'Agenzia delle entrate, l'elenco dei soggetti tenuti al versamento del contributo.

6. A decorrere dal 2024, nelle more delle procedure concorsuali per l'assunzione del personale di cui al comma 5 e fino al termine delle procedure di reclutamento, l'Autorità provvede all'esercizio dei compiti derivanti dalla designazione di cui al presente articolo mediante l'utilizzazione di personale, nel limite massimo di 10 unità, posto in posizione di comando, distacco, fuori ruolo o aspettativa o in analoghe posizioni secondo i rispettivi ordinamenti, ai sensi dell'articolo 17, comma 14, della legge 15 maggio 1997, n. 127. Per la durata del collocamento fuori ruolo è reso indisponibile un numero di posti nella dotazione organica dell'amministrazione di provenienza equivalente dal punto di vista finanziario. Il personale di cui al primo periodo, non rientrante nella pianta organica dell'Autorità, è individuato a seguito di apposito interpellato, in cui sono specificati i profili professionali richiesti, cui possono aderire i dipendenti appartenenti ai ruoli delle amministrazioni pubbliche di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, con esclusione del personale docente, educativo, amministrativo, tecnico e ausiliario delle istituzioni scolastiche, e mantiene il trattamento economico fondamentale delle amministrazioni di appartenenza, compresa l'indennità di amministrazione, i cui oneri restano a carico delle stesse. L'Autorità provvede agli oneri del trattamento economico accessorio mediante i contributi previsti al comma 5.».

— Si riporta il testo dell'articolo 8 del citato decreto-legge 14 giugno 2021, n. 82, come modificato dalla presente legge:

«Art. 8 (Nucleo per la cybersicurezza). — 1. Presso l'Agenzia è costituito, in via permanente, il Nucleo per la cybersicurezza, a supporto del Presidente del Consiglio dei ministri nella materia della cybersicurezza, per gli aspetti relativi alla prevenzione e preparazione ad eventuali situazioni di crisi e per l'attivazione delle procedure di allertamento.

2. Il Nucleo per la cybersicurezza è presieduto dal direttore generale dell'Agenzia o, per sua delega, dal vice direttore generale ed è composto dal Consigliere militare del Presidente del Consiglio dei ministri, da un rappresentante, rispettivamente, del DIS, dell'Agenzia informazioni e sicurezza esterna (AISE), di cui all'articolo 6 della legge 3 agosto 2007, n. 124, dell'Agenzia informazioni e sicurezza interna (AISI), di cui all'articolo 7 della legge n. 124 del 2007, di ciascuno dei Ministeri rappresentati nel CIC e del Dipartimento della protezione civile della Presidenza del Consiglio dei ministri, nonché dell'Agenzia per l'Italia digitale (AgID). Per gli aspetti relativi alla trattazione di informazioni classificate il Nucleo è integrato da un rappresentante dell'Ufficio centrale per la segretezza di cui all'articolo 9 della legge n. 124 del 2007.

3. I componenti del Nucleo possono farsi assistere alle riunioni da altri rappresentanti delle rispettive amministrazioni in relazione alle materie oggetto di trattazione. In base agli argomenti delle riunioni possono anche essere chiamati a partecipare rappresentanti di altre amministrazioni, di università o di enti e istituti di ricerca, nonché di operatori privati interessati alla materia della cybersicurezza.

4. Il Nucleo può essere convocato in composizione ristretta con la partecipazione dei rappresentanti delle sole amministrazioni e soggetti interessati, anche relativamente ai compiti di gestione delle crisi di cui all'articolo 10.

4.1. In relazione a specifiche questioni di particolare rilevanza concernenti i compiti di cui all'articolo 9, comma 1, lettera a), il Nucleo può essere convocato nella composizione di cui al comma 4 del presente articolo, di volta in volta estesa alla partecipazione di un rappresentante della Direzione nazionale antimafia e antiterrorismo, della Banca d'Italia o di uno o più operatori di cui all'articolo 1, comma 2-bis, del decreto-legge perimetrio, nonché di eventuali altri soggetti, interessati alle stesse questioni. Le amministrazioni e i soggetti convocati partecipano alle suddette riunioni a livello di vertice.».

4-bis. Ai componenti del Nucleo non spettano compensi, gettoni di presenza, rimborsi di spese o altri emolumenti comunque denominati.».

Note all'art. 22:

— Si riporta il testo dell'articolo 5, comma 1, del decreto legislativo 27 dicembre 2023, n. 209, recante: «Attuazione della riforma



fiscale in materia di fiscalità internazionale», pubblicato nella *Gazzetta Ufficiale* n. 3 del 4 gennaio 2013, come modificato dalla presente legge:

«Art. 5 (Nuovo regime agevolativo a favore dei lavoratori impatriati). — 1. I redditi di lavoro dipendente, i redditi assimilati a quelli di lavoro dipendente, i redditi di lavoro autonomo derivanti dall'esercizio di arti e professioni prodotti in Italia da lavoratori che trasferiscono la residenza nel territorio dello Stato ai sensi dell'articolo 2 del testo unico delle imposte sui redditi di cui al decreto del Presidente della Repubblica 22 dicembre 1986, n. 917, entro il limite annuo di 600.000 euro concorrono alla formazione del reddito complessivo limitatamente al 50 per cento del loro ammontare al ricorrere delle seguenti condizioni:

a) i lavoratori si impegnano a risiedere fiscalmente in Italia per un periodo di tempo corrispondente a quello di cui al comma 3, secondo periodo;

b) i lavoratori non sono stati fiscalmente residenti in Italia nei tre periodi d'imposta precedenti il loro trasferimento. Se il lavoratore presta l'attività lavorativa nel territorio dello Stato in favore dello stesso soggetto presso il quale è stato impiegato all'estero prima del trasferimento oppure in favore di un soggetto appartenente al suo stesso gruppo, il requisito minimo di permanenza all'estero è di:

1) sei periodi d'imposta, se il lavoratore non è stato in precedenza impiegato in Italia in favore dello stesso soggetto oppure di un soggetto appartenente al suo stesso gruppo;

2) sette periodi d'imposta, se il lavoratore, prima del suo trasferimento all'estero, è stato impiegato in Italia in favore dello stesso soggetto oppure di un soggetto appartenente al suo stesso gruppo;

c) l'attività lavorativa è prestata per la maggior parte del periodo d'imposta nel territorio dello Stato;

d) i lavoratori sono in possesso dei requisiti di elevata qualificazione o specializzazione come definiti dal decreto legislativo 28 giugno 2012, n. 108 e dal decreto legislativo 9 novembre 2007, n. 206, oppure hanno svolto un'attività di ricerca anche applicata nell'ambito delle tecnologie di intelligenza artificiale.

Omissis.

— Si riporta l'articolo 6, del decreto 22 ottobre 2004, n. 270, recante: «Modifiche al regolamento recante norme concernenti l'autonomia didattica degli atenei, approvato con decreto del Ministro dell'università e della ricerca scientifica e tecnologica 3 novembre 1999, n. 509», pubblicato nella *Gazzetta Ufficiale* 12 novembre 2004, n. 266:

«Art. 6 (Requisiti di ammissione ai corsi di studio). — 1. Per essere ammessi ad un corso di laurea occorre essere in possesso di un diploma di scuola secondaria superiore o di altro titolo di studio conseguito all'estero, riconosciuto idoneo. I regolamenti didattici di ateneo, ferme restando le attività di orientamento, coordinate e svolte ai sensi dell'articolo 11, comma 7, lettera g), richiedono altresì il possesso o l'acquisizione di un'adeguata preparazione iniziale. A tal fine gli stessi regolamenti didattici definiscono le conoscenze richieste per l'accesso e ne determinano le modalità di verifica, anche a conclusione di attività formative propedeutiche, svolte eventualmente in collaborazione con istituti di istruzione secondaria superiore. Se la verifica non è positiva vengono indicati specifici obblighi formativi aggiuntivi da soddisfare nel primo anno di corso. Tali obblighi formativi aggiuntivi sono assegnati anche agli studenti dei corsi di laurea ad accesso programmato che siano stati ammessi ai corsi con una votazione inferiore ad una prefissata votazione minima.

2. Per essere ammessi ad un corso di laurea magistrale occorre essere in possesso della laurea o del diploma universitario di durata triennale, ovvero di altro titolo di studio conseguito all'estero, riconosciuto idoneo. Nel caso di corsi di laurea magistrale per i quali non sia previsto il numero programmato dalla normativa vigente in materia di accessi ai corsi universitari, l'università stabilisce per ogni corso di laurea magistrale, specifici criteri di accesso che prevedono, comunque, il possesso di requisiti curriculari e l'adeguatezza della personale preparazione verificata dagli atenei, con modalità definite nei regolamenti didattici. L'iscrizione ai corsi di laurea magistrale può essere consentita dall'università anche ad anno accademico iniziato, purché in tempo utile per la partecipazione ai corsi nel rispetto delle norme stabilite nei regolamenti stessi.

3. In deroga al comma 2, e all'articolo 7, comma 2, i decreti ministeriali possono prevedere l'ammissione ad un corso di laurea magistrale con il possesso del diploma di scuola secondaria superiore, esclusivamente per corsi di studio regolati da normative dell'Unione europea che non prevedano, per tali corsi, titoli universitari di primo livello, ovvero, fermo restando il periodo formativo iniziale comune di cui all'articolo 11, comma 7, lettera a), per i corsi di studio finalizzati all'accesso alle professioni legali.

4. Per essere ammessi ad un corso di specializzazione occorre essere in possesso almeno della laurea, ovvero di altro titolo di studio conseguito all'estero, riconosciuto idoneo. Nel rispetto delle norme e delle direttive di cui all'articolo 3, comma 6, i decreti ministeriali stabiliscono gli specifici requisiti di ammissione ad un corso di specializzazione, ivi compresi gli eventuali crediti formativi universitari aggiuntivi rispetto al titolo di studio già conseguito.

5. Per essere ammessi ad un corso di dottorato di ricerca occorre essere in possesso della laurea magistrale ovvero di altro titolo di studio conseguito all'estero e riconosciuto idoneo.

6. Il riconoscimento dell'idoneità dei titoli di studio conseguiti all'estero ai soli fini dell'ammissione a corsi di studio e di dottorato di ricerca è deliberata dall'università interessata, nel rispetto degli accordi internazionali vigenti.»

Note all'art. 23:

— Si riporta il testo dei commi 116 e 209, della legge 30 dicembre 2018, n. 145, recante: «Bilancio di previsione dello Stato per l'anno finanziario 2019 e bilancio pluriennale per il triennio 2019-2021», pubblicata nella *Gazzetta Ufficiale* n. 302 del 31 dicembre 2012:

«116. Al fine di semplificare e rafforzare il settore del venture capital e il tessuto economico-produttivo del Paese, il Ministero dello sviluppo economico può autorizzare la cessione, a condizioni di mercato, da parte dell'Agenzia nazionale per l'attrazione degli investimenti e lo sviluppo d'impresa Spa - Invitalia, di una quota di partecipazione, anche di controllo, detenuta nella società di gestione del risparmio Invitalia Ventures SGR Spa - Invitalia SGR, nonché di una quota di partecipazione in fondi da essa gestiti, per favorire la gestione sinergica delle risorse di cui all'articolo 23 del decreto-legge 22 giugno 2012, n. 83, convertito, con modificazioni, dalla legge 7 agosto 2012, n. 134, all'articolo 1, comma 897, della legge 27 dicembre 2017, n. 205, e al comma 121 del presente articolo, già affidate a Invitalia SGR, e a condizione che dalla cessione derivi l'apporto di risorse aggiuntive da parte del soggetto acquirente. Con direttiva del Ministro dello sviluppo economico a Invitalia sono stabiliti i contenuti e i termini della cessione, anche ai fini dell'esercizio del diritto di opzione di cui al comma 117, unitamente ai criteri di governance per l'esercizio dei diritti di azionista sull'eventuale quota di minoranza e di titolare di quote dei fondi di investimento.»

«209. Per le finalità di cui al comma 206, è istituito, nello stato di previsione del Ministero dello sviluppo economico, il Fondo di sostegno al Venture Capital con una dotazione di 30 milioni di euro per ciascuno degli anni 2019, 2020 e 2021 e di 5 milioni di euro per ciascuno degli anni dal 2022 al 2025.»

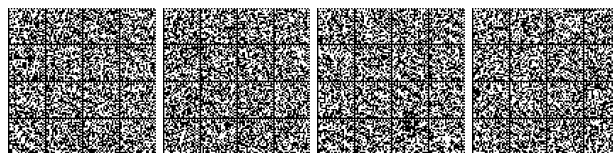
Note all'art. 24:

— Si riporta il testo degli articoli 31 e 32 della legge 24 dicembre 2012, n. 234, recante: «Norme generali sulla partecipazione dell'Italia alla formazione e all'attuazione della normativa e delle politiche dell'Unione europea», pubblicata nella *Gazzetta Ufficiale* n. 3 del 4 gennaio 2013:

«Art. 31 (Procedure per l'esercizio delle deleghe legislative conferite al Governo con la legge di delegazione europea). — 1. In relazione alle deleghe legislative conferite con la legge di delegazione europea per il recepimento delle direttive, il Governo adotta i decreti legislativi entro il termine di quattro mesi antecedenti a quello di recepimento indicato in ciascuna delle direttive; per le direttive il cui termine così determinato sia già scaduto alla data di entrata in vigore della legge di delegazione europea, ovvero scada nei tre mesi successivi, il Governo adotta i decreti legislativi di recepimento entro tre mesi dalla data di entrata in vigore della medesima legge; per le direttive che non prevedono un termine di recepimento, il Governo adotta i relativi decreti legislativi entro dodici mesi dalla data di entrata in vigore della legge di delegazione europea.

2. I decreti legislativi sono adottati, nel rispetto dell'articolo 14 della legge 23 agosto 1988, n. 400, su proposta del Presidente del Consiglio dei Ministri o del Ministro per gli affari europei e del Ministro con competenza prevalente nella materia, di concerto con i Ministri degli affari esteri, della giustizia, dell'economia e delle finanze e con gli altri Ministri interessati in relazione all'oggetto della direttiva. I decreti legislativi sono accompagnati da una tabella di concordanza tra le disposizioni in essi previste e quelle della direttiva da recepire, predisposta dall'amministrazione con competenza istituzionale prevalente nella materia.

3. La legge di delegazione europea indica le direttive in relazione alle quali sugli schemi dei decreti legislativi di recepimento è acquisito il parere delle competenti Commissioni parlamentari della Camera dei deputati e del Senato della Repubblica. In tal caso gli schemi dei decreti



legislativi sono trasmessi, dopo l'acquisizione degli altri pareri previsti dalla legge, alla Camera dei deputati e al Senato della Repubblica affinché su di essi sia espresso il parere delle competenti Commissioni parlamentari. Decorsi quaranta giorni dalla data di trasmissione, i decreti sono emanati anche in mancanza del parere. Qualora il termine per l'espressione del parere parlamentare di cui al presente comma ovvero i diversi termini previsti dai commi 4 e 9 scadano nei trenta giorni che precedono la scadenza dei termini di delega previsti ai commi 1 o 5 o successivamente, questi ultimi sono prorogati di tre mesi.

4. Gli schemi dei decreti legislativi recanti recepimento delle direttive che comportino conseguenze finanziarie sono corredati della relazione tecnica di cui all'articolo 17, comma 3, della legge 31 dicembre 2009, n. 196. Su di essi è richiesto anche il parere delle Commissioni parlamentari competenti per i profili finanziari. Il Governo, ove non intenda conformarsi alle condizioni formulate con riferimento all'esigenza di garantire il rispetto dell'articolo 81, quarto comma, della Costituzione, ritrasmette alle Camere i testi, corredati dei necessari elementi integrativi d'informazione, per i pareri definitivi delle Commissioni parlamentari competenti per i profili finanziari, che devono essere espressi entro venti giorni.

5. Entro ventiquattro mesi dalla data di entrata in vigore di ciascuno dei decreti legislativi di cui al comma 1, nel rispetto dei principi e criteri direttivi fissati dalla legge di delegazione europea, il Governo può adottare, con la procedura indicata nei commi 2, 3 e 4, disposizioni integrative e correttive dei decreti legislativi emanati ai sensi del citato comma 1, fatto salvo il diverso termine previsto dal comma 6.

6. Con la procedura di cui ai commi 2, 3 e 4 il Governo può adottare disposizioni integrative e correttive di decreti legislativi emanati ai sensi del comma 1, al fine di recepire atti delegati dell'Unione europea di cui all'articolo 290 del Trattato sul funzionamento dell'Unione europea, che modificano o integrano direttive recepite con tali decreti legislativi. Le disposizioni integrative e correttive di cui al primo periodo sono adottate nel termine di cui al comma 5 o nel diverso termine fissato dalla legge di delegazione europea. Resta ferma la disciplina di cui all'articolo 36 per il recepimento degli atti delegati dell'Unione europea che recano meri adeguamenti tecnici.

7. I decreti legislativi di recepimento delle direttive previste dalla legge di delegazione europea, adottati, ai sensi dell'articolo 117, quinto comma, della Costituzione, nelle materie di competenza legislativa delle regioni e delle province autonome, si applicano alle condizioni e secondo le procedure di cui all'articolo 41, comma 1.

8. I decreti legislativi adottati ai sensi dell'articolo 33 e attinenti a materie di competenza legislativa delle regioni e delle province autonome sono emanati alle condizioni e secondo le procedure di cui all'articolo 41, comma 1.

9. Il Governo, quando non intende conformarsi ai pareri parlamentari di cui al comma 3, relativi a sanzioni penali contenute negli schemi di decreti legislativi recanti attuazione delle direttive, ritrasmette i testi, con le sue osservazioni e con eventuali modificazioni, alla Camera dei deputati e al Senato della Repubblica. Decorsi venti giorni dalla data di ritrasmissione, i decreti sono emanati anche in mancanza di nuovo parere.

Art. 32 (*Principi e criteri direttivi generali di delega per l'attuazione del diritto dell'Unione europea*). — 1. Salvi gli specifici principi e criteri direttivi stabiliti dalla legge di delegazione europea e in aggiunta a quelli contenuti nelle direttive da attuare, i decreti legislativi di cui all'articolo 31 sono informati ai seguenti principi e criteri direttivi generali:

a) le amministrazioni direttamente interessate provvedono all'attuazione dei decreti legislativi con le ordinarie strutture amministrative, secondo il principio della massima semplificazione dei procedimenti e delle modalità di organizzazione e di esercizio delle funzioni e dei servizi;

b) ai fini di un migliore coordinamento con le discipline vigenti per i singoli settori interessati dalla normativa da attuare, sono introdotte le occorrenti modificazioni alle discipline stesse, anche attraverso il riassetto e la semplificazione normativi con l'indicazione esplicita delle norme abrogate, fatti salvi i procedimenti oggetto di semplificazione amministrativa ovvero le materie oggetto di delegificazione;

c) gli atti di recepimento di direttive dell'Unione europea non possono prevedere l'introduzione o il mantenimento di livelli di regolazione superiori a quelli minimi richiesti dalle direttive stesse, ai sensi dell'articolo 14, commi 24-bis, 24-ter e 24-quater, della legge 28 novembre 2005, n. 246;

d) al di fuori dei casi previsti dalle norme penali vigenti, ove necessario per assicurare l'osservanza delle disposizioni contenute nei decreti legislativi, sono previste sanzioni amministrative e penali per le infrazioni alle disposizioni dei decreti stessi. Le sanzioni penali, nei limiti, rispettivamente, dell'ammenda fino a 150.000 euro e dell'arresto fino a tre anni, sono previste, in via alternativa o congiunta, solo nei casi in cui le infrazioni ledano o espongano a pericolo interessi costituzionalmente protetti. In tali casi sono previste: la pena dell'ammenda alternativa all'arresto per le infrazioni che espongano a pericolo o danneggino l'interesse protetto; la pena dell'arresto congiunta a quella dell'ammenda per le infrazioni che rechino un danno di particolare gravità. Nelle predette ipotesi, in luogo dell'arresto e dell'ammenda, possono essere previste anche le sanzioni alternative di cui agli articoli 53 e seguenti del decreto legislativo 28 agosto 2000, n. 274, e la relativa competenza del giudice di pace. La sanzione amministrativa del pagamento di una somma non inferiore a 150 euro e non superiore a 150.000 euro è prevista per le infrazioni che ledono o espongono a pericolo interessi diversi da quelli indicati dalla presente lettera. Nell'ambito dei limiti minimi e massimi previsti, le sanzioni indicate dalla presente lettera sono determinate nella loro entità, tenendo conto della diversa potenzialità lesiva dell'interesse protetto che ciascuna infrazione presenta in astratto, di specifiche qualità personali del colpevole, comprese quelle che impongono particolari doveri di prevenzione, controllo o vigilanza, nonché del vantaggio patrimoniale che l'infrazione può recare al colpevole ovvero alla persona o all'ente nel cui interesse egli agisce. Ove necessario per assicurare l'osservanza delle disposizioni contenute nei decreti legislativi, sono previste inoltre le sanzioni amministrative accessorie della sospensione fino a sei mesi e, nei casi più gravi, della privazione definitiva di facoltà e diritti derivanti da provvedimenti dell'amministrazione, nonché sanzioni penali accessorie nei limiti stabiliti dal codice penale. Al medesimo fine è prevista la confisca obbligatoria delle cose che servono o furono destinate a commettere l'illecito amministrativo o il reato previsti dai medesimi decreti legislativi, nel rispetto dei limiti stabiliti dall'articolo 240, terzo e quarto comma, del codice penale e dall'articolo 20 della legge 24 novembre 1981, n. 689, e successive modificazioni. Entro i limiti di pena indicati nella presente lettera sono previste sanzioni anche accessorie identiche a quelle eventualmente già comminate dalle leggi vigenti per violazioni omogenee e di pari offensività rispetto alle infrazioni alle disposizioni dei decreti legislativi. Nelle materie di cui all'articolo 117, quarto comma, della Costituzione, le sanzioni amministrative sono determinate dalle regioni;

e) al recepimento di direttive o all'attuazione di altri atti dell'Unione europea che modificano precedenti direttive o atti già attuati con legge o con decreto legislativo si procede, se la modificazione non comporta ampliamento della materia regolata, apportando le corrispondenti modificazioni alla legge o al decreto legislativo di attuazione della direttiva o di altro atto modificato;

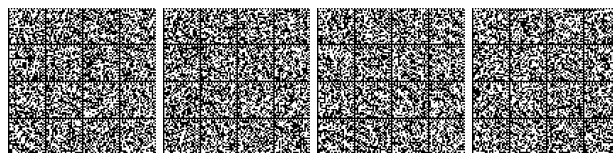
f) nella redazione dei decreti legislativi di cui all'articolo 31 si tiene conto delle eventuali modificazioni delle direttive dell'Unione europea comunque intervenute fino al momento dell'esercizio della delega;

g) quando si verificano sovrapposizioni di competenze tra amministrazioni diverse o comunque siano coinvolte le competenze di più amministrazioni statali, i decreti legislativi individuano, attraverso le più opportune forme di coordinamento, rispettando i principi di sussidiarietà, differenziazione, adeguatezza e leale collaborazione e le competenze delle regioni e degli altri enti territoriali, le procedure per salvaguardare l'unitarietà dei processi decisionali, la trasparenza, la celerità, l'efficacia e l'economicità nell'azione amministrativa e la chiara individuazione dei soggetti responsabili;

h) qualora non siano di ostacolo i diversi termini di recepimento, vengono attuate con un unico decreto legislativo le direttive che riguardano le stesse materie o che comunque comportano modifiche degli stessi atti normativi;

i) è assicurata la parità di trattamento dei cittadini italiani rispetto ai cittadini degli altri Stati membri dell'Unione europea e non può essere previsto in ogni caso un trattamento sfavorevole dei cittadini italiani.»

— Si riporta il testo dell'articolo 8, del decreto legislativo 28 agosto 1997, n. 281, recante: «Definizione ed ampliamento delle attribuzioni della Conferenza permanente per i rapporti tra lo Stato, le regioni e le province autonome di Trento e Bolzano ed unificazione, per le materie ed i compiti di interesse comune delle regioni, delle province e dei co-



muni, con la Conferenza Stato - città ed autonomie locali», pubblicato nella *Gazzetta Ufficiale* 30 agosto 1997, n. 202:

«Art. 8 (*Conferenza Stato-città ed autonomie locali e Conferenza unificata*). — 1. La Conferenza Stato-città ed autonomie locali è unificata per le materie ed i compiti di interesse comune delle regioni, delle province, dei comuni e delle comunità montane, con la Conferenza Stato-regioni.

2. La Conferenza Stato-città ed autonomie locali è presieduta dal Presidente del Consiglio dei Ministri o, per sua delega, dal Ministro dell'interno o dal Ministro per gli affari regionali nella materia di rispettiva competenza; ne fanno parte altresì il Ministro del tesoro e del bilancio e della programmazione economica, il Ministro delle finanze, il Ministro dei lavori pubblici, il Ministro della sanità, il presidente dell'Associazione nazionale dei comuni d'Italia - ANCI, il presidente dell'Unione province d'Italia - UPI ed il presidente dell'Unione nazionale comuni, comunità ed enti montani - UNCEM. Ne fanno parte inoltre quattordici sindaci designati dall'ANCI e sei presidenti di provincia designati dall'UPI. Dei quattordici sindaci designati dall'ANCI cinque rappresentano le città individuate dall'articolo 17 della legge 8 giugno 1990, n. 142. Alle riunioni possono essere invitati altri membri del Governo, nonché rappresentanti di amministrazioni statali, locali o di enti pubblici.

3. La Conferenza Stato-città ed autonomie locali è convocata almeno ogni tre mesi, e comunque in tutti i casi il presidente ne ravvisa la necessità o qualora ne faccia richiesta il presidente dell'ANCI, dell'UPI o dell'UNCEM.

4. La Conferenza unificata di cui al comma 1 è convocata dal Presidente del Consiglio dei Ministri. Le sedute sono presiedute dal Presidente del Consiglio dei Ministri o, su sua delega, dal Ministro per gli affari regionali o, se tale incarico non è conferito, dal Ministro dell'interno.»

— Per i riferimenti al regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024 si vedano le note all'articolo 1.

— Si riporta il testo dell'articolo 3, della legge 14 gennaio 2013, n. 4, recante: «Disposizioni in materia di professioni non organizzate», pubblicata nella *Gazzetta Ufficiale* 26 gennaio 2013, n. 22:

«Art. 3 (*Forme aggregative delle associazioni*). — 1. Le associazioni professionali di cui all'art. 2, mantenendo la propria autonomia, possono riunirsi in forme aggregative da esse costituite come associazioni di natura privatistica.

2. Le forme aggregative rappresentano le associazioni aderenti e agiscono in piena indipendenza e imparzialità.

3. Le forme aggregative hanno funzioni di promozione e qualificazione delle attività professionali che rappresentano, nonché di divulgazione delle informazioni e delle conoscenze ad esse connesse e di rappresentanza delle istanze comuni nelle sedi politiche e istituzionali. Su mandato delle singole associazioni, esse possono controllare l'operato delle medesime associazioni, ai fini della verifica del rispetto e della congruità degli standard professionali e qualitativi dell'esercizio dell'attività e dei codici di condotta definiti dalle stesse associazioni.»

— La legge 24 novembre 1981, n. 689, recante: «Modifiche al sistema penale», è pubblicata nella *Gazzetta Ufficiale* n. 329 del 30 novembre 1981.

— Si riporta il testo dell'articolo 17, comma 4-*quater*, del citato decreto-legge 14 giugno 2021, n. 82:

«Art. 17 (*Disposizioni transitorie e finali*). — *Omissis*.

4-*quater*. La disciplina del procedimento sanzionatorio amministrativo dell'Agenzia è definita con regolamento che stabilisce, in particolare, termini e modalità per l'accertamento, la contestazione e la notificazione delle violazioni della normativa in materia di cybersicurezza e l'irrogazione delle relative sanzioni di competenza dell'Agenzia ai sensi del presente decreto e delle altre disposizioni che assegnano poteri accertativi e sanzionatori all'Agenzia. Il regolamento di cui al primo periodo è adottato, entro novanta giorni dalla data di entrata in vigore della presente disposizione, con decreto del Presidente del Consiglio dei ministri, anche in deroga all'articolo 17 della legge 23 agosto 1988, n. 400, sentito il Comitato interministeriale per la cybersicurezza e acquisito il parere delle competenti Commissioni parlamentari. Fino alla data di entrata in vigore del regolamento di cui al presente comma, ai procedimenti sanzionatori si applicano, per ciascuna fase procedimentale di cui al primo periodo, le disposizioni contenute nelle sezioni I e II del capo I della legge 24 novembre 1981, n. 689.

Omissis».

Note all'art. 25:

— Si riporta il testo dell'articolo 1 della legge 22 aprile 1941, n. 633, recante: «Protezione del diritto d'autore e di altri diritti connessi al suo esercizio», pubblicata nella *Gazzetta Ufficiale* n. 166 del 16 luglio 1941, come modificato dalla presente legge:

«Art. 1. — Sono protette ai sensi di questa legge le opere dell'ingegno umano di carattere creativo che appartengono alla letteratura, alla musica, alle arti figurative, all'architettura, al teatro ed alla cinematografia, qualunque ne sia il modo o la forma di espressione, anche laddove create con l'ausilio di strumenti di intelligenza artificiale, purché costituenti risultato del lavoro intellettuale dell'autore.

Sono altresì protetti i programmi per elaboratore come opere letterarie ai sensi della Convenzione di Berna sulla protezione delle opere letterarie ed artistiche ratificata e resa esecutiva con legge 20 giugno 1978, n. 399, nonché le banche di dati che per la scelta o la disposizione del materiale costituiscono una creazione intellettuale dell'autore.»

Note all'art. 26:

— Si riporta il testo degli articoli 61 e 294 codice penale, come modificato dalla presente legge:

Art. 61. — Circostanze aggravanti comuni o circostanze aggravanti speciali, le circostanze seguenti:

1° l'aver agito per motivi abietti o futili;

2° l'aver commesso il reato per eseguirne od occultarne un altro, ovvero per conseguire o assicurare a sé o ad altri il prodotto o il profitto o il prezzo ovvero la impunità di un altro reato;

3° l'aver, nei delitti colposi, agito nonostante la previsione dell'evento;

4° l'aver adoperato sevizie, o l'aver agito con crudeltà verso le persone;

5° l'aver profittato di circostanze di tempo, di luogo o di persona, anche in riferimento all'età, tali da ostacolare la pubblica o privata difesa;

6° l'aver il colpevole commesso il reato durante il tempo, in cui si è sottratto volontariamente alla esecuzione di un mandato o di un ordine di arresto o di cattura o di carcerazione, spedito per un precedente reato;

7° l'aver, nei delitti contro il patrimonio, o che comunque offendono il patrimonio, ovvero nei delitti determinati da motivi di lucro, cagionato alla persona offesa dal reato un danno patrimoniale di rilevante gravità;

8° l'aver aggravato o tentato di aggravare le conseguenze del delitto commesso;

9° l'aver commesso il fatto con abuso dei poteri, o con violazione dei doveri inerenti a una pubblica funzione o a un pubblico servizio, ovvero alla qualità di ministro di un culto;

10° l'aver commesso il fatto contro un pubblico ufficiale o una persona incaricata di un pubblico servizio, o rivestita della qualità di ministro del culto cattolico o di un culto ammesso nello Stato, ovvero contro un agente diplomatico o consolare di uno Stato estero, nell'atto o a causa dell'adempimento delle funzioni o del servizio;

11° l'aver commesso il fatto con abuso di autorità o di relazioni domestiche, ovvero con abuso di relazioni di ufficio, di prestazione d'opera, di coabitazione, o di ospitalità.

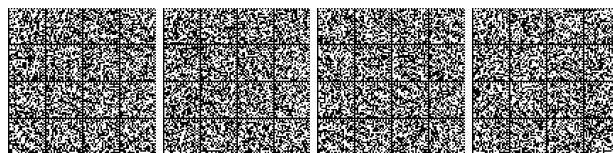
11-bis. l'aver il colpevole commesso il fatto mentre si trova illegalmente sul territorio nazionale.

11-ter) l'aver commesso un delitto contro la persona ai danni di un soggetto minore all'interno o nelle adiacenze di istituti di istruzione o di formazione.

11-quater. l'aver il colpevole commesso un delitto non colposo durante il periodo in cui era ammesso ad una misura alternativa alla detenzione in carcere.

11-quinquies) l'aver, nei delitti non colposi contro la vita e l'incolumità individuale e contro la libertà personale, commesso il fatto in presenza o in danno di un minore di anni diciotto ovvero in danno di persona in stato di gravidanza.

11-sexies) l'aver, nei delitti non colposi, commesso il fatto in danno di persone ricoverate presso strutture sanitarie o presso strutture sociosanitarie residenziali o semiresidenziali, pubbliche o private, ovvero presso strutture socio-educative.



11-septies) l'aver commesso il fatto in occasione o a causa di manifestazioni sportive o durante i trasferimenti da o verso i luoghi in cui si svolgono dette manifestazioni.

11-octies) l'aver agito, nei delitti commessi con violenza o minaccia, in danno degli esercenti le professioni sanitarie e socio-sanitarie nonché di chiunque svolga attività ausiliarie di cura, assistenza sanitaria o soccorso, funzionali allo svolgimento di dette professioni, a causa o nell'esercizio di tali professioni o attività.

11-novies) l'aver agito, nei delitti commessi con violenza o minaccia, in danno di un dirigente scolastico o di un membro del personale docente, educativo, amministrativo, tecnico o ausiliario della scuola, a causa o nell'esercizio delle loro funzioni.

11-decies) *l'aver commesso il fatto mediante l'impiego di sistemi di intelligenza artificiale, quando gli stessi, per la loro natura o per le modalità di utilizzo, abbiano costituito mezzo insidioso, ovvero quando il loro impiego abbia comunque ostacolato la pubblica o la privata difesa, ovvero aggravato le conseguenze del reato.*».

«Art. 294 (Attentati contro i diritti politici del cittadino). — Chiunque con violenza, minaccia o inganno impedisce in tutto o in parte l'esercizio di un diritto politico, ovvero determina taluno a esercitarlo in senso difforme dalla sua volontà, è punito con la reclusione da uno a cinque anni. *La pena è della reclusione da due a sei anni se l'inganno è posto in essere mediante l'impiego di sistemi di intelligenza artificiale.*».

— Si riporta il testo dell'articolo 2637 codice civile, come modificato dalla presente legge:

«Art. 2637 (Aggiotaggio). — Chiunque diffonde notizie false, ovvero pone in essere operazioni simulate o altri artifici concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari non quotati o per i quali non è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato, ovvero ad incidere in modo significativo sull'affidamento che il pubblico ripone nella stabilità patrimoniale di banche o di gruppi bancari, è punito con la pena della reclusione da uno a cinque anni. *La pena è della reclusione da due a sette anni se il fatto è commesso mediante l'impiego di sistemi di intelligenza artificiale.*».

— Si riporta il testo dell'articolo 171 della citata legge 22 aprile 1941, n. 633, come modificato dalla presente legge:

«Art. 171. — Salvo quanto previsto dall'art. 171-bis e dall'articolo 171-ter è punito con la multa da euro 51 (lire 100.000) a euro 2.065 (lire 4 milioni) 277 chiunque senza averne diritto, a qualsiasi scopo e in qualsiasi forma:

a) riproduce, trascrive, recita in pubblico, diffonde, vende o mette in vendita o pone altrimenti in commercio un'opera altrui o ne rivela il contenuto prima che sia reso pubblico, o introduce e mette in circolazione nello Stato esemplari prodotti all'estero contrariamente alla legge italiana;

a-bis) mette a disposizione del pubblico, immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta, o parte di essa;

a-ter) *riproduce o estrae testo o dati da opere o altri materiali disponibili in rete o in banche di dati in violazione degli articoli 70-ter e 70-quater, anche attraverso sistemi di intelligenza artificiale;*

b) rappresenta, esegue o recita in pubblico o diffonde, con o senza variazioni od aggiunte, un'opera altrui adatta a pubblico spettacolo od una composizione musicale. La rappresentazione o esecuzione comprende la proiezione pubblica dell'opera cinematografica, l'esecuzione in pubblico delle composizioni musicali inserite nelle opere cinematografiche e la radiodiffusione mediante altoparlante azionato in pubblico;

c) compie i fatti indicati nelle precedenti lettere mediante una delle forme di elaborazione previste da questa legge;

d) riproduce un numero di esemplari o esegue o rappresenta un numero di esecuzioni o di rappresentazioni maggiore di quello che aveva il diritto rispettivamente di riprodurre o di rappresentare;

e) riproduce con qualsiasi processo di duplicazione dischi o altri apparecchi analoghi o li smercia, ovvero introduce nel territorio dello Stato le riproduzioni così fatte all'estero;

f) in violazione dell'art. 79 ritrasmette su filo o per radio o registra in dischi fonografici o altri apparecchi analoghi le trasmissioni o ritrasmissioni radiofoniche o smercia i dischi fonografici o altri apparecchi indebitamente registrati.

Chiunque commette la violazione di cui al primo comma, lettera a-bis), è ammesso a pagare, prima dell'apertura del dibattimento, ovvero prima dell'emissione del decreto penale di condanna, una somma corri-

spondente alla metà del massimo della pena stabilita dal primo comma per il reato commesso, oltre le spese del procedimento. Il pagamento estingue il reato.

La pena è della reclusione fine ad un anno o della multa non inferiore a lire cinquemila se i reati di cui sopra sono commessi sopra una opera altrui non destinata alla pubblicità, ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onore od alla reputazione dell'autore.

La violazione delle disposizioni di cui al terzo ed al quarto comma dell'articolo 68 comporta la sospensione della attività di fotocopia, xerocopia o analogo sistema di riproduzione da sei mesi ad un anno nonché la sanzione amministrativa pecuniaria da due a dieci milioni di lire.».

— Si riporta il testo dell'articolo 185 del decreto legislativo 24 febbraio 1998, n. 58, recante: «Testo unico delle disposizioni in materia di intermediazione finanziaria, ai sensi degli articoli 8 e 21 della legge 6 febbraio 1996, n. 52», pubblicato nella *Gazzetta Ufficiale* n. 71 del 26 marzo 1998, come modificato dalla presente legge:

«Art. 185 (Manipolazione del mercato). — 1. Chiunque diffonde notizie false o pone in essere operazioni simulate o altri artifici concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari, è punito con la reclusione da due a dodici anni e con la multa da euro ventimila a euro cinque milioni. *La pena è della reclusione da due a sette anni e della multa da euro venticinquemila a euro sei milioni se il fatto è commesso mediante l'impiego di sistemi di intelligenza artificiale.*

1-bis. Non è punibile chi ha commesso il fatto per il tramite di ordini di compravendita o operazioni effettuate per motivi legittimi e in conformità a prassi di mercato ammesse, ai sensi dell'articolo 13 del regolamento (UE) n. 596/2014.

2. Il giudice può aumentare la multa fino al triplo o fino al maggiore importo di dieci volte il prodotto o il profitto conseguito dal reato quando, per la rilevante offensività del fatto, per le qualità personali del colpevole o per l'entità del prodotto o del profitto conseguito dal reato, essa appare inadeguata anche se applicata nel massimo.

2-bis.

2-ter.».

Note all'art. 28:

— Si riporta il testo dell'articolo 7, comma 1, lettera z), del citato decreto-legge 14 giugno 2021, n. 82:

«Art. 7 (Funzioni dell'Agenzia per la cybersicurezza nazionale). — 1. L'Agenzia:

a) è Autorità nazionale per la cybersicurezza e, in relazione a tale ruolo, assicura, nel rispetto delle competenze attribuite dalla normativa vigente ad altre amministrazioni, ferme restando le attribuzioni del Ministro dell'interno in qualità di autorità nazionale di pubblica sicurezza, ai sensi della legge 1° aprile 1981, n. 121, il coordinamento tra i soggetti pubblici coinvolti in materia di cybersicurezza a livello nazionale e promuove la realizzazione di azioni comuni dirette ad assicurare la sicurezza e la resilienza cibernetiche per lo sviluppo della digitalizzazione del Paese, del sistema produttivo e delle pubbliche amministrazioni, nonché per il conseguimento dell'autonomia, nazionale ed europea, riguardo a prodotti e processi informatici di rilevanza strategica a tutela degli interessi nazionali nel settore. Per le reti, i sistemi informativi e i servizi informatici attinenti alla gestione delle informazioni classificate restano fermi sia quanto previsto dal regolamento adottato ai sensi dell'articolo 4, comma 3, lettera l), della legge n. 124 del 2007, sia le competenze dell'Ufficio centrale per la segretezza di cui all'articolo 9 della medesima legge n. 124 del 2007;

b) predisporre la strategia nazionale di cybersicurezza;

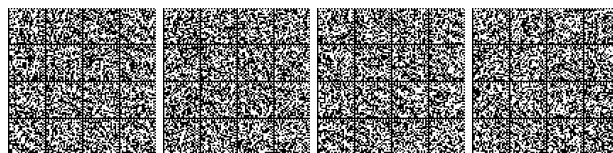
c) svolge ogni necessaria attività di supporto al funzionamento del Nucleo per la cybersicurezza, di cui all'articolo 8;

d) è Autorità nazionale competente NIS e Punto di contatto unico NIS di cui all'articolo 2, comma 1, lettere d) ed e), del decreto legislativo NIS, a tutela dell'unità giuridica dell'ordinamento;

d-bis) è Autorità nazionale di gestione delle crisi informatiche di cui all'articolo 2, comma 1, lettera g), del decreto legislativo NIS;

d-ter) è CSIRT nazionale, denominato CSIRT Italia, di cui all'articolo 2, comma 1, lettera i), del decreto legislativo NIS;

e) è Autorità nazionale di certificazione della cybersicurezza ai sensi dell'articolo 58 del regolamento (UE) 2019/881 del Parlamento



europeo e del Consiglio, del 17 aprile 2019, e assume tutte le funzioni in materia di certificazione di sicurezza cibernetica già attribuite al Ministero dello sviluppo economico dall'ordinamento vigente, comprese quelle relative all'accertamento delle violazioni e all'irrogazione delle sanzioni; nello svolgimento dei compiti di cui alla presente lettera:

1) accredita, ai sensi dell'articolo 60, paragrafo 1, del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, le strutture specializzate del Ministero della difesa e del Ministero dell'interno quali organismi di valutazione della conformità per i sistemi di rispettiva competenza;

2) delega, ai sensi dell'articolo 56, paragrafo 6, lettera b), del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, il Ministero della difesa e il Ministero dell'interno, attraverso le rispettive strutture accreditate di cui al numero 1) della presente legge, al rilascio del certificato europeo di sicurezza cibernetica;

e-bis) è Autorità competente per l'esecuzione dei compiti previsti dal regolamento delegato (UE) 2024/1366 della Commissione, dell'11 marzo 2024, che integra il regolamento (UE) 2019/943 del Parlamento europeo e del Consiglio

f) assume tutte le funzioni in materia di cybersicurezza già attribuite dalle disposizioni vigenti al Ministero dello sviluppo economico, ivi comprese quelle relative:

1) al perimetro di sicurezza nazionale cibernetica, di cui al decreto-legge perimetro e ai relativi provvedimenti attuativi, ivi incluse le funzioni attribuite al Centro di valutazione e certificazione nazionale ai sensi del decreto-legge perimetro, le attività di ispezione e verifica di cui all'articolo 1, comma 6, lettera c), del decreto-legge perimetro e quelle relative all'accertamento delle violazioni e all'irrogazione delle sanzioni amministrative previste dal medesimo decreto, fatte salve quelle di cui all'articolo 3 del regolamento adottato con decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131;

2) alla sicurezza e all'integrità delle comunicazioni elettroniche, di cui agli articoli 16-bis e 16-ter del decreto legislativo 1° agosto 2003, n. 259, e relative disposizioni attuative;

3) alla sicurezza delle reti e dei sistemi informativi, di cui al decreto legislativo NIS;

g) partecipa, per gli ambiti di competenza, al gruppo di coordinamento istituito ai sensi dei regolamenti di cui all'articolo 1, comma 8, del decreto-legge 15 marzo 2012, n. 21, convertito, con modificazioni, dalla legge 11 maggio 2012, n. 56;

h) assume tutte le funzioni attribuite alla Presidenza del Consiglio dei ministri in materia di perimetro di sicurezza nazionale cibernetica, di cui al decreto-legge perimetro e ai relativi provvedimenti attuativi, ivi incluse le attività di ispezione e verifica di cui all'articolo 1, comma 6, lettera c), del decreto-legge perimetro e quelle relative all'accertamento delle violazioni e all'irrogazione delle sanzioni amministrative previste dal medesimo decreto, fatte salve quelle di cui all'articolo 3 del regolamento adottato con decreto del Presidente del Consiglio dei ministri n. 131 del 2020;

i) assume tutte le funzioni già attribuite al Dipartimento delle informazioni per la sicurezza (DIS), di cui all'articolo 4 della legge 3 agosto 2007, n. 124, dal decreto-legge perimetro e dai relativi provvedimenti attuativi e supporta il Presidente del Consiglio dei ministri ai fini dell'articolo 1, comma 19-bis, del decreto-legge perimetro;

l) provvede, sulla base delle attività di competenza del Nucleo per la cybersicurezza di cui all'articolo 8, alle attività necessarie per l'attuazione e il controllo dell'esecuzione dei provvedimenti assunti dal Presidente del Consiglio dei ministri ai sensi dell'articolo 5 del decreto-legge perimetro;

m) assume tutte le funzioni in materia di cybersicurezza già attribuite all'Agenzia per l'Italia digitale dalle disposizioni vigenti e, in particolare, quelle di cui all'articolo 51 del decreto legislativo 7 marzo 2005, n. 82, nonché quelle in materia di adozione di linee guida contenenti regole tecniche di cybersicurezza ai sensi dell'articolo 71 del medesimo decreto legislativo. L'Agenzia assume, altresì, i compiti di cui all'articolo 33-septies, comma 4, del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, già attribuiti all'Agenzia per l'Italia digitale;

m-bis) provvede, anche attraverso un'apposita sezione nell'ambito della strategia di cui alla lettera b), allo sviluppo e alla diffusione di standard, linee guida e raccomandazioni al fine di rafforzare la cybersicurezza dei sistemi informatici, alla valutazione della sicurezza dei sistemi crittografici nonché all'organizzazione e alla gestione di attività di divulgazione finalizzate a promuovere l'utilizzo della crittografia,

fia, anche a vantaggio della tecnologia blockchain, come strumento di cybersicurezza. L'Agenzia, anche per il rafforzamento dell'autonomia industriale e tecnologica dell'Italia, promuove altresì la collaborazione con centri universitari e di ricerca per la valorizzazione dello sviluppo di nuovi algoritmi proprietari, la ricerca e il conseguimento di nuove capacità crittografiche nazionali nonché la collaborazione internazionale con gli organismi esteri che svolgono analoghe funzioni. A tale fine, è istituito presso l'Agenzia, nell'ambito delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente e senza nuovi o maggiori oneri a carico della finanza pubblica, il Centro nazionale di crittografia, il cui funzionamento è disciplinato con provvedimento del direttore generale dell'Agenzia stessa. Il Centro nazionale di crittografia svolge le funzioni di centro di competenza nazionale per tutti gli aspetti della crittografia in ambito non classificato, ferme restando le competenze dell'Ufficio centrale per la segretezza, di cui all'articolo 9 della legge 3 agosto 2007, n. 124, con riferimento alle informazioni e alle attività previste dal regolamento adottato ai sensi dell'articolo 4, comma 3, lettera l), della citata legge n. 124 del 2007, nonché le competenze degli organismi di cui agli articoli 4, 6 e 7 della medesima legge;

m-ter) provvede alla qualificazione dei servizi cloud per la pubblica amministrazione nel rispetto della disciplina dell'Unione europea e del regolamento di cui all'articolo 33-septies, comma 4, del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221;

n) sviluppa capacità nazionali di prevenzione, monitoraggio, rilevamento, analisi e risposta, per prevenire e gestire gli incidenti di sicurezza informatica e gli attacchi informatici, anche attraverso il CSIRT Italia di cui all'articolo 2, comma 1, lettera i) del decreto legislativo NIS. A tale fine, promuove iniziative di partenariato pubblico-privato per rendere effettive tali capacità;

n-bis) nell'ambito delle funzioni di cui al primo periodo della lettera n), svolge ogni attività diretta all'analisi e al supporto per il contenimento e il ripristino dell'operatività dei sistemi compromessi, con la collaborazione dei soggetti pubblici o privati che hanno subito incidenti di sicurezza informatica o attacchi informatici. La mancata collaborazione di cui al primo periodo è valutata ai fini dell'applicazione delle sanzioni previste dall'articolo 1, commi 10 e 14, del decreto-legge perimetro, per i soggetti di cui all'articolo 1, comma 2-bis, del medesimo decreto-legge perimetro, i soggetti essenziali e i soggetti importanti di cui all'articolo 6 del decreto legislativo NIS, del decreto legislativo NIS e di cui all'articolo 40, comma 3, alinea, del codice delle comunicazioni elettroniche, di cui al decreto legislativo 1° agosto 2003, n. 259; restano esclusi gli organi dello Stato preposti alla prevenzione, all'accertamento e alla repressione dei reati, alla tutela dell'ordine e della sicurezza pubblica e alla difesa e sicurezza militare dello Stato, nonché gli organismi di informazione per la sicurezza di cui agli articoli 4, 6 e 7 della legge 3 agosto 2007, n. 124;

n-ter) provvede alla raccolta, all'elaborazione e alla classificazione dei dati relativi alle notifiche di incidenti ricevute dai soggetti che a ciò siano tenuti in osservanza delle disposizioni vigenti. Tali dati sono resi pubblici nell'ambito della relazione prevista dall'articolo 14, comma 1, quali dati ufficiali di riferimento degli attacchi informatici portati ai soggetti che operano nei settori rilevanti per gli interessi nazionali nel campo della cybersicurezza. Agli adempimenti previsti dalla presente lettera si provvede con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente;

o) partecipa alle esercitazioni nazionali e internazionali che riguardano la simulazione di eventi di natura cibernetica al fine di innalzare la resilienza del Paese;

p) cura e promuove la definizione ed il mantenimento di un quadro giuridico nazionale aggiornato e coerente nel dominio della cybersicurezza, tenendo anche conto degli orientamenti e degli sviluppi in ambito internazionale. A tal fine, l'Agenzia esprime pareri non vincolanti sulle iniziative legislative o regolamentari concernenti la cybersicurezza;

q) coordina, in raccordo con il Ministero degli affari esteri e della cooperazione internazionale, la cooperazione internazionale nella materia della cybersicurezza. Nell'ambito dell'Unione europea e a livello internazionale, l'Agenzia cura i rapporti con i competenti organismi, istituzioni ed enti, nonché segue nelle competenti sedi istituzionali le tematiche di cybersicurezza, fatta eccezione per gli ambiti in cui la legge attribuisce specifiche competenze ad altre amministrazioni. In tali casi, è comunque assicurato il raccordo con l'Agenzia al fine di garantire posizioni nazionali unitarie e coerenti con le politiche di cybersicurezza definite dal Presidente del Consiglio dei ministri;



r) perseguendo obiettivi di eccellenza, supporta negli ambiti di competenza, mediante il coinvolgimento del sistema dell'università e della ricerca nonché del sistema produttivo nazionali, lo sviluppo di competenze e capacità industriali, tecnologiche e scientifiche. A tali fini, l'Agenzia può promuovere, sviluppare e finanziare specifici progetti ed iniziative, volti anche a favorire il trasferimento tecnologico dei risultati della ricerca nel settore.

L'Agenzia assicura il necessario raccordo con le altre amministrazioni a cui la legge attribuisce competenze in materia di cybersicurezza e, in particolare, con il Ministero della difesa per gli aspetti inerenti alla ricerca militare. L'Agenzia può altresì promuovere la costituzione di aree dedicate allo sviluppo dell'innovazione finalizzate a favorire la formazione e il reclutamento di personale nei settori avanzati dello sviluppo della cybersicurezza, nonché promuovere la realizzazione di studi di fattibilità e di analisi valutative finalizzati a tale scopo;

s) stipula accordi bilaterali e multilaterali, anche mediante il coinvolgimento del settore privato e industriale, con istituzioni, enti e organismi di altri Paesi per la partecipazione dell'Italia a programmi di cybersicurezza, assicurando il necessario raccordo con le altre amministrazioni a cui la legge attribuisce competenze in materia di cybersicurezza, ferme restando le competenze del Ministero degli affari esteri e della cooperazione internazionale;

t) promuove, sostiene e coordina la partecipazione italiana a progetti e iniziative dell'Unione europea e internazionali, anche mediante il coinvolgimento di soggetti pubblici e privati nazionali, nel campo della cybersicurezza e dei correlati servizi applicativi, ferme restando le competenze del Ministero degli affari esteri e della cooperazione internazionale. L'Agenzia assicura il necessario raccordo con le altre amministrazioni a cui la legge attribuisce competenze in materia di cybersicurezza e, in particolare, con il Ministero della difesa per gli aspetti inerenti a progetti e iniziative in collaborazione con la NATO e con l'Agenzia europea per la difesa;

u) svolge attività di comunicazione e promozione della consapevolezza in materia di cybersicurezza, al fine di contribuire allo sviluppo di una cultura nazionale in materia;

v) promuove la formazione, la crescita tecnico-professionale e la qualificazione delle risorse umane nel campo della cybersicurezza, in particolare favorendo l'attivazione di percorsi formativi universitari in materia, anche attraverso l'assegnazione di borse di studio, di dottorato e assegni di ricerca, sulla base di apposite convenzioni con soggetti pubblici e privati; nello svolgimento di tali compiti, l'Agenzia può avvalersi anche delle strutture formative e delle capacità della Presidenza del Consiglio dei ministri, del Ministero della difesa e del Ministero dell'interno, secondo termini e modalità da definire con apposito decreto del Presidente del Consiglio dei ministri, di concerto con i Ministri interessati;

v-bis) può predisporre attività di formazione specifica riservate ai giovani che aderiscono al servizio civile regolate sulla base di apposite convenzioni. In ogni caso, il servizio prestato è, a tutti gli effetti, riconosciuto come servizio civile;

z) per le finalità di cui al presente articolo, può concludere accordi di collaborazione, comunque denominati, con soggetti privati, costituire e partecipare a partenariati pubblico-privato nel territorio nazionale, nonché, previa autorizzazione del Presidente del Consiglio dei ministri, a consorzi, fondazioni o società con soggetti pubblici e privati, italiani o di Paesi appartenenti all'Unione europea. Sulla base dell'interesse nazionale e previa autorizzazione del Presidente del Consiglio dei ministri, può altresì partecipare a consorzi, fondazioni o società con soggetti pubblici e privati di Paesi della NATO ovvero di Paesi extraeuropei con i quali siano stati sottoscritti accordi di cooperazione o di partenariato per lo sviluppo di sistemi di intelligenza artificiale.

aa) è designata quale Centro nazionale di coordinamento ai sensi dell'articolo 6 del regolamento (UE) 2021/887 del Parlamento europeo e del Consiglio del 20 maggio 2021, che istituisce il Centro europeo di competenza per la cybersicurezza nell'ambito industriale, tecnologico e della ricerca e la rete dei centri nazionali di coordinamento.

1-bis. Anche ai fini dell'esercizio delle funzioni di cui al comma 1, lettere r), s), t), u), v), z) e aa), presso l'Agenzia è istituito, con funzioni di consulenza e di proposta, un Comitato tecnico-scientifico, presieduto dal direttore generale della medesima Agenzia, o da un dirigente da lui delegato, e composto da personale della stessa Agenzia e da qualificati rappresentanti dell'industria, degli enti di ricerca, dell'accademia e delle associazioni del settore della sicurezza, desi-

gnati con decreto del Presidente del Consiglio dei ministri. La composizione e l'organizzazione del Comitato tecnico-scientifico sono disciplinate secondo le modalità e i criteri definiti dal regolamento di cui all'articolo 6, comma 1.

Per la partecipazione al Comitato tecnico-scientifico non sono previsti gettoni di presenza, compensi o rimborsi di spese.

2. Nell'ambito dell'Agenzia sono nominati, con decreto del Presidente del Consiglio dei ministri, il rappresentante nazionale, e il suo sostituto, nel Consiglio di direzione del Centro europeo di competenza per la cybersicurezza nell'ambito industriale, tecnologico e della ricerca, ai sensi dell'articolo 12 del regolamento (UE) 2021/887.

3.

4. Il Centro di valutazione e certificazione nazionale, istituito presso il Ministero dello sviluppo economico, è trasferito presso l'Agenzia.

5. Nel rispetto delle competenze del Garante per la protezione dei dati personali, l'Agenzia, per le finalità di cui al presente decreto, consulta il Garante e collabora con esso, anche in relazione agli incidenti che comportano violazioni di dati personali. L'Agenzia e il Garante possono stipulare appositi protocolli d'intenti che definiscono altresì le modalità della loro collaborazione nell'ambito delle risorse disponibili a legislazione vigente e senza nuovi o maggiori oneri per la finanza pubblica».

— Si riporta il testo degli articoli 1 della legge 28 giugno 2024 n. 901, recante: «Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici», pubblicata nella *Gazzetta Ufficiale* 2 luglio 2024, n. 153, come modificato dalla presente legge:

«Art. 1 (*Obblighi di notifica di incidenti*). — 1. Le pubbliche amministrazioni centrali individuate ai sensi dell'articolo 1, comma 3, della legge 31 dicembre 2009, n. 196, le regioni e le province autonome di Trento e di Bolzano, le città metropolitane, i comuni con popolazione superiore a 100.000 abitanti e, comunque, i comuni capoluoghi di regione, nonché le società di trasporto pubblico urbano con bacino di utenza non inferiore a 100.000 abitanti, le società di trasporto pubblico extraurbano operanti nell'ambito delle città metropolitane e le aziende sanitarie locali segnalano e notificano, con le modalità e nei termini di cui al comma 2 del presente articolo, gli incidenti indicati nella tassonomia adottata con determinazione tecnica del direttore generale dell'Agenzia per la cybersicurezza nazionale, aventi impatto su reti, sistemi informativi e servizi informatici. Tra i soggetti di cui al presente comma sono altresì comprese le rispettive società in house che forniscono servizi informatici, i servizi di trasporto di cui al primo periodo del presente comma ovvero servizi di raccolta, smaltimento o trattamento di acque reflue urbane, domestiche o industriali, come definite ai sensi dell'articolo 2, punti 1), 2) e 3), della direttiva 91/271/CEE del Consiglio, del 21 maggio 1991, o di gestione dei rifiuti, come definita ai sensi dell'articolo 3, punto 9), della direttiva 2008/98/CE del Parlamento europeo e del Consiglio, del 19 novembre 2008.

2. I soggetti di cui al comma 1 segnalano, senza ritardo e comunque entro il termine massimo di ventiquattro ore dal momento in cui ne sono venuti a conoscenza a seguito delle evidenze comunque ottenute, qualunque incidente riconducibile a una delle tipologie individuate nella tassonomia di cui al comma 1 ed effettuano, entro settantadue ore a decorrere dal medesimo momento, la notifica completa di tutti gli elementi informativi disponibili. La segnalazione e la successiva notifica sono effettuate tramite le apposite procedure disponibili nel sito internet istituzionale dell'Agenzia per la cybersicurezza nazionale.

3. Per i comuni con popolazione superiore a 100.000 abitanti e i comuni capoluoghi di regione, per le società di trasporto pubblico urbano con bacino di utenza non inferiore a 100.000 abitanti, per le società di trasporto pubblico extraurbano operanti nell'ambito delle città metropolitane, per le aziende sanitarie locali e per le società in house che forniscono servizi informatici, i servizi di trasporto di cui al presente comma ovvero servizi di raccolta, smaltimento o trattamento di acque reflue urbane, domestiche o industriali, come definite ai sensi dell'articolo 2, punti 1), 2) e 3), della direttiva 91/271/CEE del Consiglio, del 21 maggio 1991, o di gestione dei rifiuti, come definita ai sensi dell'articolo 3, punto 9), della direttiva 2008/98/CE del Parlamento europeo e del Consiglio, del 19 novembre 2008, gli obblighi di cui ai commi 1 e 2 del presente articolo si applicano a decorrere dal centottantesimo giorno successivo alla data di entrata in vigore della presente legge.

4. Qualora i soggetti di cui al comma 1 effettuino notifiche volontarie di incidenti al di fuori dei casi indicati nella tassonomia di cui al medesimo comma 1, si applicano le disposizioni dell'articolo 18, commi 3, 4 e 5, del decreto legislativo 18 maggio 2018, n. 65.



5. Nel caso di inosservanza dell'obbligo di notifica di cui ai commi 1 e 2, l'Agenzia per la cybersicurezza nazionale comunica all'interessato che la reiterazione dell'inosservanza, nell'arco di cinque anni, comporterà l'applicazione delle disposizioni di cui al comma 6 e può disporre, nei dodici mesi successivi all'accertamento del ritardo o dell'omissione, l'invio di ispezioni, anche al fine di verificare l'attuazione, da parte dei soggetti interessati dall'incidente, di interventi di rafforzamento della resilienza agli stessi, direttamente indicati dall'Agenzia per la cybersicurezza nazionale ovvero previsti da apposite linee guida adottate dalla medesima Agenzia. Le modalità di tali ispezioni sono disciplinate con determinazione del direttore generale dell'Agenzia per la cybersicurezza nazionale, pubblicata nella *Gazzetta Ufficiale*.

6. Nei casi di reiterata inosservanza, nell'arco di cinque anni, dell'obbligo di notifica di cui ai commi 1 e 2, l'Agenzia per la cybersicurezza nazionale applica altresì, nel rispetto delle disposizioni dell'articolo 17, comma 4-*quater*, del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, introdotto dall'articolo 11 della presente legge, una sanzione amministrativa pecuniaria da euro 25.000 a euro 125.000 a carico dei soggetti di cui al comma 1 del presente articolo. La violazione delle disposizioni del comma 1 del presente articolo può costituire causa di responsabilità disciplinare e amministrativo-contabile per i funzionari e i dirigenti responsabili.

7. Fermi restando gli obblighi e le sanzioni, anche penali, previsti da altre norme di legge, le disposizioni del presente articolo non si applicano:

a) ai soggetti di cui all'articolo 3, comma 1, lettere g) e i), del decreto legislativo 18 maggio 2018, n. 65, e a quelli di cui all'articolo 1, comma 2-*bis*, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133;

b) agli organi dello Stato preposti alla prevenzione, all'accertamento e alla repressione dei reati, alla tutela dell'ordine e della sicurezza pubblica e alla difesa e sicurezza militare dello Stato e agli organismi di informazione per la sicurezza di cui agli articoli 4, 6 e 7 della legge 3 agosto 2007, n. 124.».

25G00143

