Roberto GAROFOLI

# CODICE AMMINISTRATIVO

aggiornamento a cura di
Sara PIANCASTELLI

Neldiritto Editore

2025
XV edizione

settori ordinari, purché l'importo stimato della parte del contratto che costituisce un appalto, calcolato secondo il presente articolo, sia pari o superiore alla soglia pertinente.

22. Nel caso di appalti il cui oggetto rientra in parte nei settori ordinari e in parte nei settori speciali, le disposizioni applicabili sono determinate dai commi seguenti, fatta salva la facoltà di cui al comma 20.

23. Se le diverse parti di un determinato contratto sono oggettivamente non separabili, il regime giuridico applicabile è determinato in base all'oggetto principale del contratto in questione.

24. Nei settori speciali, nel caso di contratti aventi ad oggetto prestazioni strumentali a più attività, le stazioni appaltanti possono scegliere di aggiudicare appalti distinti per ogni attività o di aggiudicare un appalto unico. Se le stazioni appaltanti scelgono di aggiudicare appalti distinti, il regime giuridico applicabile a ciascuno di essi è determinato in base all'attività cui è strumentale. Se le stazioni appaltanti decidono di aggiudicare un appalto unico, si applicano i commi 25 e 26. La decisione di aggiudicare un unico appalto o più appalti distinti non può essere adottata allo scopo di escludere l'appalto o gli appalti dall'ambito di applicazione del codice.

25. A un appalto avente ad oggetto prestazioni strumentali all'esercizio di più attività si applicano le disposizioni relative alla principale attività cui la prestazione è destinata.

26. Nel caso di appalti aventi ad oggetto prestazioni per cui è oggettivamente impossibile stabilire a quale attività esse siano principalmente strumentali, le disposizioni applicabili sono determinate come segue:

a) l'appalto è aggiudicato secondo le disposizioni del codice che disciplinano gli appalti nei settori ordinari se una delle attività è disciplinata dalle disposizioni relative all'aggiudicazione degli appalti nei settori ordinari e l'altra dalle disposizioni relative all'aggiudicazione degli appalti nei settori speciali;

b) l'appalto è aggiudicato secondo le disposizioni del codice che disciplinano gli appalti nei settori speciali se una delle attività è disciplinata dalle disposizioni relative all'aggiudicazione degli appalti nei settori speciali e l'altra dalle disposizioni relative all'aggiudicazione delle concessioni;

c) l'appalto è aggiudicato secondo le disposizioni del codice che disciplinano gli appalti nei settori speciali se una delle attività è disciplinata dalle disposizioni relative all'aggiudicazione degli appalti nei settori speciali e l'altra non è soggetta a tali disposizioni, né a quelle relative all'aggiudicazione degli appalti nei settori ordinari o alle disposizioni relative all'aggiudicazione delle concessioni.

27. Nel caso di contratti misti che contengono elementi di appalti di forniture, lavori e servizi nei settori speciali e di concessioni, il contratto misto è aggiudicato in conformità alle disposizioni del codice che disciplinano gli appalti nei settori speciali, purché l'importo stimato della parte del contratto che costituisce un appalto disciplinato da tali disposizioni, calcolato secondo il presente articolo, sia pari o superiore alla soglia pertinente.

28. Per i contratti misti concernenti aspetti di difesa e sicurezza si applica l'articolo 137.

29. Per i contratti misti di concessione si applica l'articolo 180.

(1) *Comma modificato dall'articolo 3, comma 1, del D.Lgs. 31 dicembre **2024**, n. 209.*

**15. Responsabile unico del progetto (RUP).** — 1. Nel primo atto di avvio dell'intervento pubblico da realizzare mediante un contratto le stazioni appaltanti e gli enti concedenti nominano nell'interesse proprio o di altre amministrazioni un responsabile unico del progetto (RUP) per le fasi di programmazione, progettazione, affidamento e per l'esecuzione di ciascuna procedura soggetta al codice.

2. Le stazioni appaltanti e gli enti concedenti nominano il RUP tra i dipendenti assunti anche a tempo determinato della stazione appaltante o dell'ente concedente, preferibilmente in servizio presso l'unità organizzativa titolare del potere di spesa, in possesso dei requisiti di cui all'allegato I.2 e di competenze professionali adeguate in relazione ai compiti al medesimo affidati, nel rispetto dell'inquadramento contrattuale e delle relative mansioni. Le stazioni appaltanti e gli enti concedenti che non sono pubbliche amministrazioni o enti pubblici individuano, secondo i propri ordinamenti, uno o più soggetti cui affidare i compiti del RUP, limitatamente al rispetto delle norme del codice alla cui osservanza sono tenute. Resta in ogni caso ferma la possibilità per le stazioni appaltanti, in caso di accertata carenza nel proprio organico di personale in possesso dei requisiti di cui all'allegato I.2., di nominare il RUP tra i dipendenti di altre amministrazioni pubbliche. L'ufficio di RUP è obbligatorio e non può essere rifiutato. In caso di mancata nomina del RUP nell'atto di avvio dell'intervento pubblico, l'incarico è svolto dal responsabile dell'unità organizzativa competente per l'intervento(1).

3. Il nominativo del RUP è indicato nel bando o nell'avviso di indizione della gara, o, in mancanza, nell'invito a presentare un'offerta o nel provvedimento di affidamento diretto.

4. Ferma restando l'unicità del RUP, le stazioni appaltanti e gli enti concedenti possono individuare modelli organizzativi, i quali prevedano la nomina di un responsabile di procedimento per le fasi di programmazione, progettazione ed esecuzione e un responsabile di procedimento per la fase di affidamento. Le relative responsabilità sono ripartite in base ai compiti svolti in ciascuna fase, ferme restando le funzioni di supervisione, indirizzo e coordinamento del RUP.

5. Il RUP assicura il completamento dell'intervento pubblico nei termini previsti e nel rispetto degli obiettivi connessi al suo incarico, svolgendo tutte le attività indicate nell'allegato I.2, o che siano comunque necessarie, ove non di competenza di altri organi. [*In sede di prima applicazione del codice, l'allegato I.2 è abrogato a decorrere dalla data di entrata in vigore di un corrispondente regolamento adottato ai sensi dell'articolo 17, comma 3, della legge 23 agosto 1988, n. 400, con decreto del Ministro delle infrastrutture e dei trasporti, che lo sostituisce integralmente anche in qualità di allegato al codice.*](2)

6. Le stazioni appaltanti e gli enti concedenti possono istituire una struttura di supporto al RUP, e possono destinare risorse finanziarie non superiori all'1 per cento dell'importo posto a base di gara per l'affidamento diretto da parte del RUP di incarichi di assi-

stenza al medesimo.

7. Le stazioni appaltanti e gli enti concedenti, in coerenza con il programma degli acquisti di beni e servizi e del programma dei lavori pubblici di cui all'articolo 37, adottano un piano di formazione per il personale che svolge funzioni relative alle procedure in materia di acquisiti di lavori, servizi e forniture.

8. Negli appalti pubblici di lavori aggiudicati con la formula del contraente generale e nelle altre formule di partenariato pubblico-privato, è vietata l'attribuzione dei compiti di RUP, responsabile dei lavori, direttore dei lavori o collaudatore allo stesso contraente generale, al soggetto aggiudicatario dei contratti di partenariato pubblico-privato e ai soggetti a essi collegati.

9. Le centrali di committenza e le aggregazioni di stazioni appaltanti designano un RUP per le attività di propria competenza con i compiti e le funzioni determinate dalla specificità e complessità dei processi di acquisizione gestiti direttamente.

(1) *Comma modificato dall'articolo 4, comma 1, del D.Lgs. 31 dicembre* ***2024****, n. 209.*
(2) *Comma modificato dall'articolo 72, comma 2, lettera a), del D.Lgs. 31 dicembre* ***2024****, n. 209.*

**16. Conflitto di interessi.** — 1. Si ha conflitto di interessi quando un soggetto che, a qualsiasi titolo, interviene con compiti funzionali nella procedura di aggiudicazione o nella fase di esecuzione degli appalti o delle concessioni e ne può influenzare, in qualsiasi modo, il risultato, gli esiti e la gestione, ha direttamente o indirettamente un interesse finanziario, economico o altro interesse personale che può essere percepito come una minaccia [*concreta ed effettiva*] alla sua imparzialità e indipendenza nel contesto della procedura di aggiudicazione o nella fase di esecuzione(1).

2. In coerenza con il principio della fiducia e per preservare la funzionalità dell'azione amministrativa, la percepita minaccia all'imparzialità e indipendenza deve essere provata da chi invoca il conflitto sulla base di presupposti specifici e documentati e deve riferirsi a interessi effettivi, la cui soddisfazione sia conseguibile solo subordinando un interesse all'altro.

3. Il personale che versa nelle ipotesi di cui al comma 1 ne dà comunicazione alla stazione appaltante o all'ente concedente e si astiene dal partecipare alla procedura di aggiudicazione e all'esecuzione.

4. Le stazioni appaltanti adottano misure adeguate per individuare, prevenire e risolvere in modo efficace ogni ipotesi di conflitto di interesse nello svolgimento delle procedure di aggiudicazione ed esecuzione degli appalti e delle concessioni e vigilano affinché gli adempimenti di cui al comma 3 siano rispettati.

(1) *Comma modificato dall'articolo 15-quater, comma 1, lettera a) del D.L. 29 settembre 2023, n. 132, convertito con modificazioni dalla Legge 27 novembre 2023, n. 170.*

**17. Fasi delle procedure di affidamento.** – – 1. Prima dell'avvio delle procedure di affidamento dei contratti pubblici le stazioni appaltanti e gli enti concedenti, con apposito atto, adottano la decisione di contrarre individuando gli elementi essenziali del contratto e i criteri di selezione degli operatori economici e delle offerte.

2. In caso di affidamento diretto, l'atto di cui al comma 1 individua l'oggetto, l'importo e il contraente, unitamente alle ragioni della sua scelta, ai requisiti di carattere generale e, se necessari, a quelli inerenti alla capacità economico-finanziaria e tecnico-professionale.

3. Le stazioni appaltanti e gli enti concedenti procedono alla pubblicazione dei documenti iniziali di gara e concludono le procedure di selezione nei termini indicati nell'allegato I.3. Il superamento dei termini costituisce silenzio inadempimento e rileva anche al fine della verifica del rispetto del dovere di buona fede, anche in pendenza di contenzioso. [*In sede di prima applicazione del codice, l'allegato I.3 è abrogato a decorrere dalla data di entrata in vigore di un corrispondente regolamento emanato ai sensi dell'articolo 17, comma 1, della legge 23 agosto 1988, n. 400, su proposta del Ministro delle infrastrutture e dei trasporti, sentito il Ministro per la pubblica amministrazione, che lo sostituisce integralmente anche in qualità di allegato al codice.*](1)

3-bis. L'allegato 1.3 indica il termine massimo che deve intercorrere tra l'approvazione del progetto e la pubblicazione del bando di gara o l'invio degli inviti a offrire (2).

4. Ogni concorrente può presentare una sola offerta, che è vincolante per il periodo indicato nel bando o nell'invito e, in caso di mancata indicazione, per centottanta giorni dalla scadenza del termine per la sua presentazione. La stazione appaltante e l'ente concedente, con atto motivato, possono chiedere agli offerenti il differimento del termine.

5. L'organo preposto alla valutazione delle offerte predispone la proposta di aggiudicazione alla migliore offerta non anomala.

L'organo competente a disporre l'aggiudicazione esamina la proposta, e, se la ritiene legittima e conforme all'interesse pubblico, dopo aver verificato il possesso dei requisiti in capo all'offerente, dispone l'aggiudicazione, che è immediatamente efficace.

6. L'aggiudicazione non equivale ad accettazione dell'offerta. L'offerta dell'aggiudicatario è irrevocabile fino al termine stabilito per la stipulazione del contratto.

7. Una volta disposta l'aggiudicazione, il contratto è stipulato secondo quanto previsto dall'articolo 18.

8. Fermo quanto previsto dall'articolo 50, comma 6, l'esecuzione del contratto può essere iniziata, anche prima della stipula, per motivate ragioni. L'esecuzione è sempre iniziata prima della stipula se sussistono le ragioni d'urgenza di cui al comma 9.

9. L'esecuzione d'urgenza è effettuata quando ricorrono eventi oggettivamente imprevedibili, per evitare situazioni di pericolo per persone, animali, cose, per l'igiene e la salute pubblica, per il patrimonio storico, artistico, culturale, ovvero nei casi in cui la mancata esecuzione immediata della prestazione dedotta nella gara determinerebbe un grave danno all'interesse pubblico che è destinata a soddisfare, ivi compresa la perdita di finanziamenti dell'Unione europea.

10. La pendenza di un contenzioso non può mai giustificare la sospensione della procedura o dell'aggiudicazione, salvi i poteri cautelari del giudice amministrativo e quelli di autotutela della stazione appaltante o dell'ente concedente, da esercitarsi da parte del dirigente competente.

(1) *Comma modificato dagli articoli 5, comma 1, lettera a) e 72, comma 2, lettera b), del D.Lgs. 31 dicembre* ***2024****, n. 209.*

# 2. D.Lgs. 4 settembre 2024, n. 138

Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (1).

(1) *In Gazz. Uff. 1° ottobre 2024, n. 230.*

## CAPO I
## Disposizioni generali

**1. Oggetto.** — 1. Il presente decreto stabilisce misure volte a garantire un livello elevato di sicurezza informatica in ambito nazionale, contribuendo ad incrementare il livello comune di sicurezza nell'Unione europea in modo da migliorare il funzionamento del mercato interno.

2. Ai fini del comma 1, il presente decreto prevede:

a) la Strategia nazionale di cybersicurezza, recante previsioni volte a garantire un livello elevato di sicurezza informatica;

b) l'integrazione del quadro di gestione delle crisi informatiche, nel contesto dell'organizzazione nazionale per la gestione delle crisi che coinvolgono aspetti di cybersicurezza, di cui all'articolo 10 del decreto-legge 4 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109;

c) la conferma dell'Agenzia per la cybersicurezza nazionale quale:

1) Autorità nazionale competente NIS, disciplinandone i poteri inerenti all'implementazione e all'attuazione del presente decreto;

2) Punto di contatto unico NIS, assicurando il raccordo nazionale e transfrontaliero;

3) Gruppo di intervento nazionale per la sicurezza informatica in caso di incidente in ambito nazionale (CSIRT Italia);

d) la designazione dell'Agenzia per la cybersicurezza nazionale, con funzioni di coordinatore ai sensi dell'articolo 9, paragrafo 2, della direttiva (UE) 2022/2555, e del Ministero della difesa, ciascuno per gli ambiti di competenza indicati all'articolo 2, comma 1, lettera g), quali Autorità nazionali di gestione delle crisi informatiche su vasta scala, assicurando la coerenza con il quadro nazionale esistente in materia di gestione generale delle crisi informatiche, fermi restando i compiti del Nucleo per la cybersicurezza di cui all'articolo 9 del decreto-legge 14 giugno 2021, n. 82;

e) l'individuazione di Autorità di settore NIS che collaborano con l'Agenzia per la cybersicurezza nazionale, supportandone le funzioni svolte quale Autorità nazionale competente NIS e Punto di contatto unico NIS;

f) l'indicazione dei criteri per l'individuazione dei soggetti a cui si applica il presente decreto e la definizione dei relativi obblighi in materia di misure di gestione dei rischi per la sicurezza informatica e di notifica di incidente;

g) l'adozione di misure in materia di cooperazione e di condivisione delle informazioni ai fini dell'applicazione del presente decreto, in particolare, attraverso la partecipazione nazionale a livello dell'Unione europea:

1) al Gruppo di cooperazione NIS tra autorità competenti NIS e tra punti di contatto unici degli Stati membri dell'Unione europea, nell'ottica di incrementare la fiducia e la collaborazione a livello unionale;

2) alla Rete delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe) al fine di sostenere la gestione coordinata a livello operativo degli incidenti e delle crisi cibernetiche su vasta scala e di garantire il regolare scambio di informazioni pertinenti tra gli Stati membri e le istituzioni, gli organi e gli organismi dell'Unione europea;

3) alla Rete di CSIRT nazionali nell'ottica di assicurare una cooperazione, sul piano tecnico, rapida ed efficace.

**2. Definizioni.** — 1. Ai fini del presente decreto si applicano le definizioni seguenti:

a) «Strategia nazionale di cybersicurezza»: il quadro coerente che prevede gli obiettivi strategici e le priorità in materia di cybersicurezza, nonché la governance per il loro conseguimento, di cui all'articolo 9;

b) «Agenzia per la cybersicurezza nazionale»: l'Agenzia per la cybersicurezza nazionale di cui all'articolo 5, comma 1, del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109;

c) «Nucleo per la cybersicurezza»: il Nucleo per la cybersicurezza di cui all'articolo 8 del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109;

d) «Autorità nazionale competente NIS»: l'Agenzia per la cybersicurezza nazionale, quale Autorità nazionale competente NIS di cui all'articolo 10, comma 1;

e) «Punto di contatto unico NIS»: l'Agenzia per la cybersicurezza nazionale, quale Punto di contatto unico NIS di cui all'articolo 10, comma 2;

f) «Autorità di settore NIS»: le Amministrazioni designate quali Autorità di settore di cui all'articolo 11, commi 1 e 2;

g) «Autorità nazionali di gestione delle crisi informatiche»: per la parte relativa alla resilienza nazionale di cui all'articolo 1 del decreto-legge n. 82 del 2021, l'Agenzia per la cybersicurezza nazionale, con funzioni di coordinatore ai sensi dell'articolo 9, paragrafo 2, della direttiva (UE) 2022/2555, e, per la parte relativa alla difesa dello Stato, il Ministero della difesa, quali Autorità nazionali responsabili della gestione degli incidenti e delle crisi di cybersicurezza su vasta scala, di cui all'articolo 9 della direttiva (UE) 2022/2555;

h) «CSIRT nazionali»: i Gruppi nazionali di risposta agli incidenti di sicurezza informatica di cui all'articolo 10, paragrafo 1, della direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022;

i) «CSIRT Italia»: il Gruppo nazionale di risposta agli incidenti di sicurezza informatica ai sensi dell'articolo 15, comma 1, operante all'interno dell'Agenzia per la cybersicurezza nazionale;

l) «Gruppo di cooperazione NIS»: il Gruppo di cooperazione di cui all'articolo 18, istituito ai sensi dell'articolo 14 della direttiva (UE) 2022/2555;

m) «EU-CyCLONe»: la Rete delle organizzazioni di collegamento per le crisi informatiche di cui all'articolo 19, istituita ai sensi dell'articolo 16 della direttiva (UE) 2022/2555;

n) «Rete di CSIRT nazionali»: la Rete di CSIRT nazionali di cui all'articolo 20, istituita ai sensi dell'articolo 15 della direttiva (UE) 2022/2555;

o) «ENISA»: l'Agenzia dell'Unione europea per la sicurezza informatica, di cui all'articolo 3 del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019;

p) «sistema informativo e di rete»:

1) una rete di comunicazione elettronica ai sensi dell'articolo 2, comma 1, lettera vv), del decreto legislativo 1° agosto 2003, n. 259;

2) qualsiasi dispositivo o gruppo di dispositivi interconnessi o collegati, uno o più dei quali eseguono, in base ad un programma, un trattamento automatico di dati digitali;

3) i dati digitali conservati, elaborati, estratti o trasmessi per mezzo di reti o dispositivi di cui ai numeri 1) e 2), per il loro funzionamento, uso, protezione e manutenzione;

q) «sicurezza dei sistemi informativi e di rete»: la capacità dei sistemi informativi e di rete di resistere, con un determinato livello di affidabilità, agli eventi che potrebbero compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o elaborati o dei servizi offerti da tali sistemi informativi e di rete o accessibili attraverso di essi;

r) «sicurezza informatica»: l'insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche, così come definito dall'articolo 2, punto 1), del regolamento (UE) 2019/881;

s) «cybersicurezza»: ferme restando le definizioni di cui alle lettere q) e r), l'insieme delle attività di cui all'articolo 1, comma 1, lettera a), del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109;

t) «incidente»: un evento che compromette la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informativi e di rete o accessibili attraverso di essi;

u) «quasi-incidente»: cd. near-miss, un evento che avrebbe potuto configurare un incidente senza che quest'ultimo si sia tuttavia verificato, ivi incluso il caso in cui l'incidente sia stato efficacemente evitato;

v) «incidente di sicurezza informatica su vasta scala»: un incidente che causa un livello di perturbazione superiore alla capacità di uno Stato membro di rispondervi o che ha un impatto significativo su almeno due Stati membri;

z) «gestione degli incidenti»: le azioni e le procedure volte a prevenire, rilevare, analizzare e contenere un incidente o a rispondervi e recuperare da esso;

aa) «rischio»: la combinazione dell'entità dell'impatto di un incidente, in termini di danno o di perturbazione, e della probabilità che quest'ultimo si verifichi;

bb) «minaccia informatica»: qualsiasi circostanza, evento o azione che potrebbe danneggiare, perturbare o avere un impatto negativo di altro tipo su sistemi informativi e di rete, sugli utenti di tali sistemi e altre persone, così come definita dall'articolo 2, punto 8), del regolamento (UE) 2019/881;

cc) «minaccia informatica significativa»: una minaccia informatica che, in base alle sue caratteristiche tecniche, si presume possa avere un grave impatto sui sistemi informativi e di rete di un soggetto o sugli utenti dei servizi erogati da un soggetto causando perdite materiali o immateriali considerevoli;

dd) «approccio multi-rischio»: cosiddetto approccio all-hazards, l'approccio alla gestione dei rischi che considera quelli derivanti da tutte le tipologie di minaccia ai sistemi informativi e di rete nonché al loro contesto fisico, quali furti, incendi, inondazioni, interruzioni, anche parziali, delle telecomunicazioni e della corrente elettrica, e in generale accessi fisici non autorizzati;

ee) «singoli punti di malfunzionamento»: cosiddetto single points of failure, singolo componente di un sistema da cui dipende il funzionamento del sistema stesso;

ff) «prodotto TIC»: un elemento o un gruppo di elementi di un sistema informativo o di rete, così come definito dall'articolo 2, punto 12), del regolamento (UE) 2019/881;

gg) «servizio TIC»: un servizio consistente interamente o prevalentemente nella trasmissione, conservazione, recupero o elaborazione di informazioni per mezzo dei sistemi informativi e di rete così come definito dall'articolo 2, punto 13), del regolamento (UE) 2019/881;

hh) «processo TIC»: un insieme di attività svolte per progettare, sviluppare, fornire o mantenere un prodotto TIC o servizio TIC, così come definito dall'articolo 2, punto 14), del regolamento (UE) 2019/881;

ii) «vulnerabilità»: un punto debole, una suscettibilità o un difetto di prodotti TIC o servizi TIC che può essere sfruttato da una minaccia informatica;

ll) «specifica tecnica»: una specifica tecnica quale definita all'articolo 2, punto 4), del regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio, del 25 ottobre 2012;

mm) «punto di interscambio internet»: cosiddetto internet exchange point (IXP), un'infrastruttura di rete che consente l'interconnessione di più di due reti indipendenti (sistemi autonomi), principalmente al fine di agevolare lo scambio del traffico internet, che fornisce interconnessione soltanto ai sistemi autonomi e che non richiede che il traffico internet che passa tra qualsiasi coppia di sistemi autonomi partecipanti passi attraverso un terzo sistema autonomo né altera o interferisce altrimenti con tale traffico;

nn) «sistema dei nomi di dominio»: cosiddetto domain name system (DNS), un sistema di nomi gerarchico e distribuito che consente l'identificazione di servizi e risorse su internet, permettendo ai dispositivi degli utenti finali di utilizzare i servizi di instradamento e connettività di internet al fine di accedere a tali servizi e risorse;

oo) «fornitore di servizi di sistema dei nomi di dominio»: un soggetto che fornisce alternativamente:

1) servizi di risoluzione dei nomi di dominio ricorsivi accessibili al pubblico per gli utenti finali di internet;