

Corso online

La nuova figura del referente cyber e l'ufficio RTD

Cosa cambia per le Amministrazioni Pubbliche

Lunedì 16 settembre 2024, ore 9.00-10.00

Docente

Ernesto Belisario

Avvocato Cassazionista. Esperto di diritto delle tecnologie e diritto amministrativo.

Curatore dei progetti lapadigitale.it e leggezzero.substack.com (Maggioli Editore)

LaGazzetta**degli**EntiLocali

— Il quotidiano della PA locale —

www.lagazzettadeglientilocali.it

Il quotidiano online della Pubblica Amministrazione

“La Gazzetta degli Enti Locali” è il quotidiano online dedicato al mondo delle Amministrazioni locali. Costantemente aggiornato con le ultime novità normative, di prassi e giurisprudenza, puntualmente commentate dalle migliori firme di settore.

Servizi inclusi:

- ❖ PA Digitale Channel (11 corsi online all'anno con Ernesto Belisario sulla transizione digitale della P.A.)
- ❖ Dossier tematici ed e-book
- ❖ Scadenziario
- ❖ Domande & Risposte
- ❖ Indirizzi operativi
- ❖ Due newsletter quotidiane di aggiornamento
- ❖ TUEL e Legge 241/1990 annotati con la prassi e giurisprudenza
- ❖ Motore di ricerca

Per informazioni

SERVIZIO CLIENTI MAGGIOLI

Tel. 0541 628200



La legge 28 giugno 2024 n. 90

La legge 28 giugno 2024 n. 90: “Disposizioni in materia di rafforzamento della cyber sicurezza nazionale e di reati informatici”

The screenshot shows the NORMATTIVA portal interface. At the top, the logo "NORMATTIVA IL PORTALE DELLA LEGGE VIGENTE" is visible, along with navigation links: Home, Il progetto, Collegamenti veloci, Legislazione Regionale, and Guida all'uso. Below the navigation bar is a search section with a text input field containing the message "In caso di problemi di visualizzazione dell'atto clicca [qui](#)". There are two search buttons: "Ricerca semplice" and "Ricerca avanzata". Below the search section, a status bar indicates "stai visualizzando l'atto" with a date selector set to "12/09/2024" and a "Cerca" button. There are also radio buttons for "originario" and "multivigente". The main content area displays the title "LEGGE 28 giugno 2024, n. 90" and the subject "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici. (24G00108)". A note indicates the entry into force date: "Entrata in vigore del provvedimento: 17/07/2024". At the bottom, there are navigation links: "< nascondi", "Articoli", "articolo successivo >", "nascondi >", "APPROFONDIMENTI", and "atti aggiornati".

La legge si compone di **24 articoli**, alcuni dei quali prevedono interventi sul Codice penale e sul Codice di procedura penale (Capo II). Tra le principali misure e novità ci sono quelle relative al **potenziamento delle infrastrutture critiche di prevenzione** e la repressione dei reati informatici, la **collaborazione internazionale** e l'attenzione al tema della formazione.

La legge 28 giugno 2024 n. 90: ambito di applicazione

La L. 90/2024 si caratterizza anche per un ambito di applicazione molto ampio: da alcune tipologie di **pubbliche amministrazioni individuate** puntualmente dalla norma (art. 1) ,fino ai **soggetti ricompresi nel Perimetro di Sicurezza Nazionale Cibernetica** e a quelli sottoposti al dettato della **Direttiva NIS** e della **Direttiva NIS2**, passando per gli **organi dello Stato** considerati ormai come centrali nel settore della cybersicurezza

La legge 28 giugno 2024 n. 90: a chi si applica?

Con riferimento alle pubbliche amministrazioni, la legge è applicabile a :

- alle **P.A. centrali** incluse nell'elenco annuale ISTAT delle pubbliche amministrazioni previsto dall'articolo 1, comma 3, della legge di contabilità e finanza pubblica (**legge n. 196 del 2009**);
- alle **regioni e le province autonome** di Trento e di Bolzano;
- alle **città metropolitane** ;
- ai comuni **con popolazione superiore a 100.000 abitanti**;
- ai comuni capoluoghi di regione;



La legge 28 giugno 2024 n. 90: a chi si applica?

- alle **società di trasporto pubblico** urbano con bacino di utenza non inferiore a 100.000 abitanti;
- alle **società di trasporto pubblico extraurbano** operanti nell'ambito delle **città metropolitane**;
- alle **aziende sanitarie locali**;
- alle **società in house** degli enti fin qui richiamati, qualora siano fornitrici di **servizi informatici**, dei **servizi di trasporto** sopra indicati, dei **servizi di raccolta, smaltimento o trattamento di acque reflue urbane, domestiche o industriali**, ovvero **servizi di gestione dei rifiuti**.



La legge 28 giugno 2024 n. 90: a chi non si applica?

Sono esclusi dall'applicazione:

- gli enti rientranti nel Perimetro nazionale di sicurezza cibernetica, già soggetti ad analoghe prescrizioni contenute nel d.l. n. 105/2019;
- 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 e agli organismi di informazione per la sicurezza.

La legge 28 giugno 2024 n. 90: I principali adempimenti per le PA

- ✓ Obbligo di notifica degli attacchi informatici all'Agenzia per la Cybersicurezza Nazionale: la prima segnalazione entro 24 ore ed entro le 72 la notifica completa (art. 1)
- ✓ Nomina di un Responsabile della Cyber Sicurezza (Art. 8)
- ✓ Gestione proattiva della sicurezza informatica

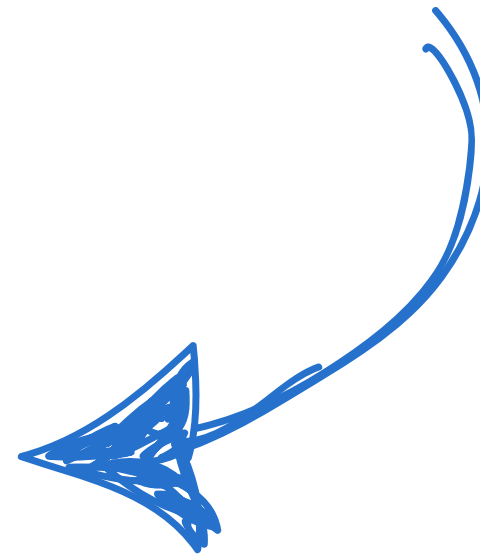
N.b: data breach e privacy

Se gli **attacchi informatici** di cui **all'articolo 1** coinvolgano o interessano **dati personali**, gli stessi hanno rilevanza anche ai fini della normativa GDPR



Data breach ex. art. 33 GDPR

L'Ente dovrà effettuare la segnalazione entro **24h ad ACN** e, nelle **72h successive**, la notifica tanto al **Garante Privacy** quanto all'**ACN**





Il referente cyber e le sue funzioni

Il referente cyber

Gli Attori Pubblici devono istituire la figura del referente per la cybersicurezza, il quale deve essere individuato in ragione delle sue specifiche professionalità e competenze possedute in materia di cybersicurezza.

Qualora l'Attore Pubblico non abbia al proprio interno un dipendente con tali requisiti, esso può **incaricare il dipendente di un altro Attore Pubblico, previa autorizzazione da parte dell'Attore Pubblico di appartenenza** e nell'ambito delle risorse disponibili a legislazione vigente senza comportare nuovi o maggiori oneri per la finanza pubblica.



Il referente cyber

La norma di riferimento è rappresentata dall'articolo 8 comma 2 della Legge 90/2024 rubricato **“Rafforzamento della resilienza delle pubbliche amministrazioni e referente per la cybersicurezza”**:

*“Presso le strutture di cui al comma 1 opera il **referente per la cybersicurezza**, individuato in ragione di **specifiche e comprovate professionalità e competenze in materia di cybersicurezza**. Qualora i soggetti di cui all'articolo 1, comma 1, non dispongano di personale dipendente fornito di tali requisiti, possono conferire l'incarico di referente per la cybersicurezza a un dipendente di una pubblica amministrazione, previa autorizzazione di quest'ultima ai sensi dell'articolo 53 del decreto legislativo 30 marzo 2001, n. 165, nell'ambito delle risorse disponibili a legislazione vigente. **Il referente per la cybersicurezza svolge anche la funzione di punto di contatto unico dell'amministrazione con l'Agenzia per la cybersicurezza nazionale** in relazione a quanto previsto dalla presente legge e dalle normative settoriali in materia di cybersicurezza cui è soggetta la medesima amministrazione. A tale fine, **il nominativo del referente per la cybersicurezza è comunicato all'Agenzia per la cybersicurezza nazionale.**”*

Il referente cyber e ACN

Il Referente, il cui nominativo deve essere **obbligatoriamente comunicato all'ACN**, svolge anzitutto la funzione di **punto di contatto unico** dell'Attore Pubblico con tale autorità in merito a quanto previsto dalla legge e dalle normative settoriali in materia di cybersecurity



The screenshot shows the official website of the Agenzia per la cybersicurezza nazionale (ACN). At the top left is the ACN logo, a circular emblem with the text 'AGENZIA PER LA CYBERSICUREZZA NAZIONALE' and 'ACN' in the center. To its right is the agency's name. A navigation bar includes links for 'Agenzia', 'PNRR', 'Cloud', 'NCC Italia', and 'Lavora con noi'. On the right, there is a button 'Segnala un incidente informatico' and a search icon. Below the navigation bar, a banner features the text 'Home / Referente per la cybersicurezza' and 'Referente per la cybersicurezza' in large white letters. The main content area contains a paragraph explaining the legal basis for the Referent role, followed by instructions on how to communicate with the ACN via PEC, including the email address acn@pec.acn.gov.it. A list of required documents is provided at the bottom. On the right side of the page, there is a vertical image showing hands typing on a laptop with digital overlays.

Agenzia per la cybersicurezza nazionale

Segnala un incidente informatico

Agenzia ▼ PNRR Cloud ▼ NCC Italia ▼ Lavora con noi

Amministrazione trasparente

Home / Referente per la cybersicurezza

Referente per la cybersicurezza

Tutti i soggetti previsti dall'articolo 1, comma 1 della Legge 28 giugno 2024, n. 90 "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici", sono tenuti a comunicare all'Agenzia la nomina del Referente per la cybersicurezza.

La comunicazione ad ACN (art. 8, comma 2) avviene inviando una PEC, attraverso il proprio domicilio digitale, all'indirizzo di posta elettronica certificata di ACN (acn@pec.acn.gov.it) e deve contenere:

- la nomina del referente per la cybersicurezza (redatta in forma libera) firmata digitalmente dal rappresentante legale del soggetto, o da persona da lui delegata (in quest'ultimo caso allegare anche la delega);
- il modulo referente per la cybersicurezza, compilato e firmato dal referente per la cybersicurezza.

Le funzioni del referente cyber

Il referente cyber provvede:

- ✓ allo sviluppo delle politiche e delle procedure di sicurezza delle informazioni;
- ✓ alla produzione e all'aggiornamento di sistemi di analisi preventiva di rilevamento e di un piano per la gestione del rischio informatico;
- ✓ alla produzione e all'aggiornamento di un documento che definisca i ruoli e l'organizzazione del sistema per la sicurezza delle informazioni dell'amministrazione;
- ✓ alla produzione e all'aggiornamento di un piano programmatico per la sicurezza di dati, sistemi e infrastrutture dell'amministrazione;

Le funzioni del referente cyber

- ✓ alla pianificazione e all'attuazione di interventi di potenziamento delle capacità per la gestione dei rischi informatici, in coerenza con i piani di cui alle lettere b) e d)
- ✓ alla pianificazione e all'attuazione dell'adozione delle misure previste dalle linee guida per la cybersicurezza emanate dall'Agenzia per la cybersicurezza nazionale;
- ✓ al monitoraggio e alla valutazione continua delle minacce alla sicurezza e delle vulnerabilità dei sistemi per il loro pronto aggiornamento di sicurezza.



I rapporti tra referente cyber e ufficio RTD

I rapporti tra referente cyber e ufficio RTD

“La struttura e il referente di cui ai commi 1 e 2 possono essere individuati, rispettivamente, nell'ufficio e nel responsabile per la transizione al digitale previsti dall'articolo 17 del codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82.”

Legge 90/2024, art. 8 comma 3

I rapporti tra referente cyber e ufficio RTD

Il legislatore precisa che:

- tale soggetto può essere individuato anche nella figura del responsabile per la transizione al digitale;
- i compiti del **referente per la cybersicurezza** possano **essere esercitati in forma associata** (art. 17, c. 1-*sexies* e 1-*septies*, del d. lgs. 82/2005)

Compiti dell'ufficio RTD

- a coordinamento strategico dello sviluppo dei sistemi informativi, di telecomunicazione e fonia, in modo da assicurare anche la coerenza con gli standard tecnici e organizzativi comuni;
- b indirizzo e coordinamento dello sviluppo dei servizi, sia interni che esterni, forniti dai sistemi informativi di telecomunicazione e fonia dell'amministrazione;



Compiti dell'ufficio RTD

- c indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza informatica relativamente ai dati, ai sistemi e alle infrastrutture anche in relazione al sistema pubblico di connettività, nel rispetto delle regole tecniche di cui all'articolo 51, comma 1
- d accesso dei soggetti disabili agli strumenti informatici e promozione dell'accessibilità anche in attuazione di quanto previsto dalla legge 9 gennaio 2004, n. 4



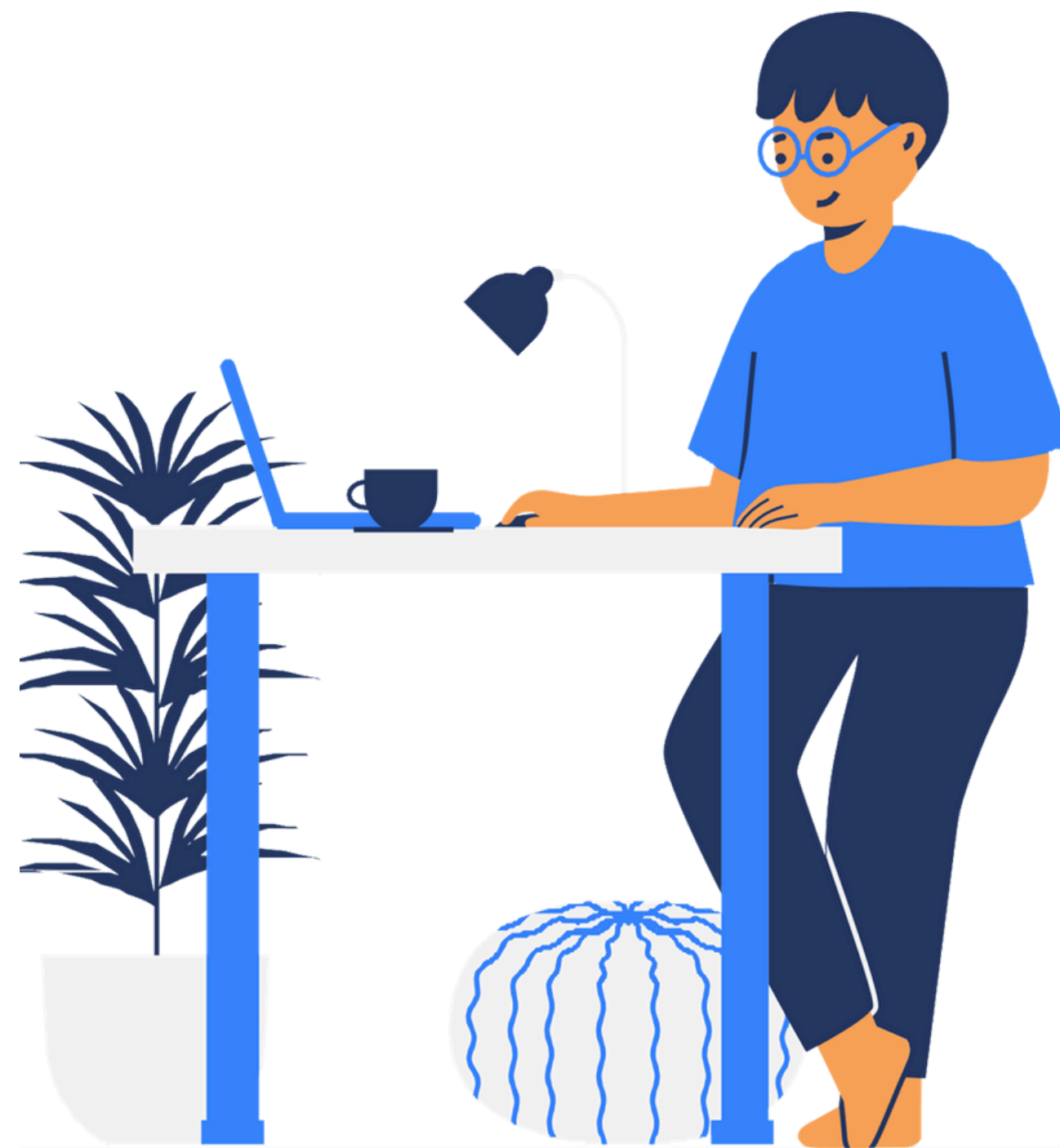
Compiti dell'ufficio RTD

- e analisi periodica della coerenza tra l'organizzazione dell'amministrazione e l'utilizzo delle tecnologie dell'informazione e della comunicazione, al fine di migliorare la soddisfazione dell'utenza e la qualità dei servizi nonché di ridurre i tempi e i costi dell'azione amministrativa
- f cooperazione alla revisione della riorganizzazione dell'amministrazione ai fini di cui alla lettera e);



Compiti dell'ufficio RTD

- g indirizzo, coordinamento e monitoraggio della pianificazione prevista per lo sviluppo e la gestione dei sistemi informativi di telecomunicazione e fonia
- h progettazione e coordinamento delle iniziative rilevanti ai fini di una più efficace erogazione di servizi in rete a cittadini e imprese mediante gli strumenti della cooperazione applicativa tra pubbliche amministrazioni, ivi inclusa la predisposizione e l'attuazione di accordi di servizio tra amministrazioni per la realizzazione e compartecipazione dei sistemi informativi cooperativi



Compiti dell'ufficio RTD



pianificazione e coordinamento degli acquisti di soluzioni e sistemi informatici, telematici e di telecomunicazione al fine di garantirne la compatibilità con gli obiettivi di attuazione dell'agenda digitale e, in particolare, con quelli stabiliti nel piano triennale di cui all'articolo 16, comma 1, lettera b).



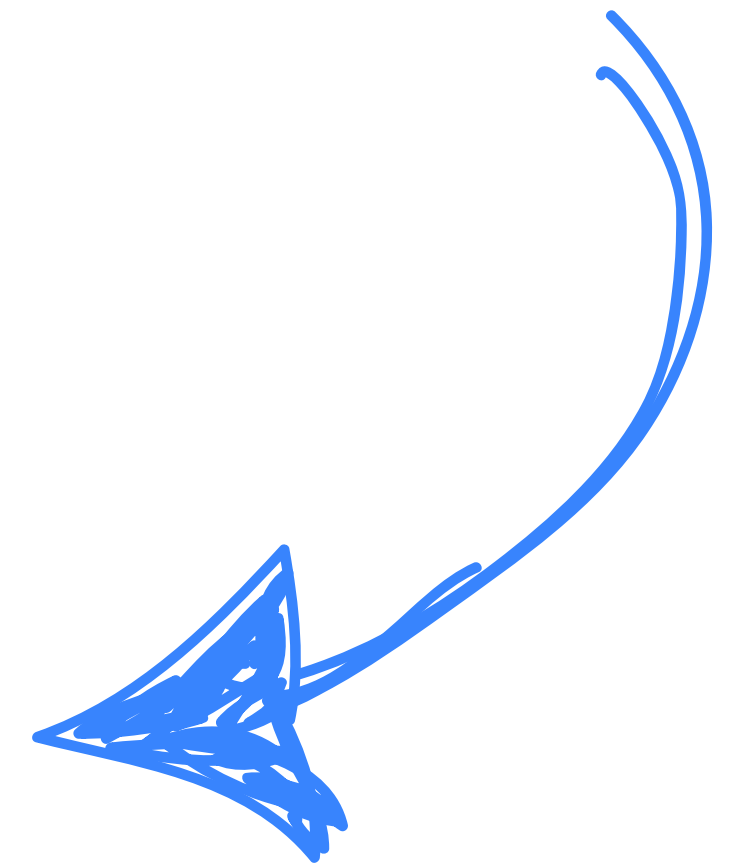


Il procurement e la tutela degli interessi nazionali strategici

I criteri di cybersecurity

Nello svolgimento delle sue funzioni, il referente dovrà adottare determinati **criteri di cybersecurity**, definiti dal legislatore come *l'insieme di criteri e regole tecniche la conformità ai quali, da parte di beni e servizi informatici da acquisire, garantisce la confidenzialità, l'integrità e la disponibilità dei dati da trattare in misura corrispondente alle esigenze di tutela degli interessi nazionali strategici*

In particolare si dispone che entro 120 giorni dall'entrata in vigore della Legge (17 luglio 2024), dovrà essere adottato un DPCM nel quale sono individuati, per specifiche categorie tecnologiche di beni e servizi informatici, gli elementi essenziali di cybersicurezza che i soggetti di cui all'articolo 2, comma 2, del codice dell'amministrazione digitale, (d.Lgs. n. 82/2005) devono tenere in considerazione



In relazione agli elementi essenziali di cybersicurezza, vengono previsti per le stazioni appaltanti, ivi incluse le centrali di committenza, i seguenti obblighi e facoltà:

- possono esercitare la facoltà di cui agli **articoli 107, comma 2, e 108, comma 10, del d.Lgs. n. 36/2023** (Codice dei contratti pubblici), se accertano che l'offerta non tiene in considerazione gli elementi essenziali di cybersicurezza individuati nel Dpcm;
- **tengono sempre in considerazione gli elementi essenziali di cybersicurezza nella valutazione dell'elemento qualitativo**, ai fini dell'individuazione del miglior rapporto qualità/prezzo per l'aggiudicazione; c) nel caso in cui sia utilizzato il criterio del minor prezzo, ai sensi dell'articolo 108, comma 3, del d.Lgs. n. 36/2023, **inseriscono gli elementi di cybersicurezza tra i requisiti minimi dell'offerta**;
- nel caso in cui sia utilizzato il **criterio dell'offerta economicamente più vantaggiosa**, ai sensi dell'articolo 108, comma 4, del codice dei Contratti, nella valutazione dell'elemento qualitativo ai fini dell'individuazione del migliore rapporto qualità/prezzo, **stabiliscono un tetto massimo per il punteggio economico entro il limite del 10%**;
- prevedono **criteri di premialità** per le proposte o per le offerte che **contemplino l'uso di tecnologie di cybersicurezza italiane o di Paesi appartenenti all'Unione europea o di Paesi aderenti alla NATO o di Paesi terzi individuati con il decreto** tra quelli che sono parte di accordi di collaborazione con l'Unione europea o con la NATO in materia di cybersicurezza.