*03 luglio 2024*

# LEGGE SULLA CYBERSICUREZZA
# TUTTI GLI ADEMPIMENTI PER LE PUBBLICHE AMMINISTRAZIONI E LE SOCIETÀ

Nella Gazzetta Ufficiale n. 153 del 02 luglio 2024 è stata pubblicata la legge n. 90 del 28 giugno 2024, la quale reca "*Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici*" (di seguito, "**Legge sulla Cybersicurezza**"), con la presente nota desideriamo fornire una descrizione dei principali adempimenti per le pubbliche amministrazioni e le società private in essa previsti.

## 1. IDENTIFICAZIONE DEI SOGGETTI RILEVANTI PER LA LEGGE SULLA CYBERSICUREZZA

La Legge sulla Cybersicurezza si rivolge ad un ampio novero di soggetti pubblici e privati. Tuttavia, ai fini della presente nota, si prendono in considerazione solo quegli obblighi e quegli adempimenti applicabili:

1. **alle pubbliche amministrazioni** a cui si rivolge il legislatore nel testo normativo, ovvero:

   - le **pubbliche amministrazioni 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);
   - le **regioni e le province autonome di Trento e di Bolzano**;
   - le **città metropolitane** (e quindi, Torino, Milano, Venezia, Genova, Bologna, Firenze, Bari, Napoli, Reggio Calabria, a cui si deve aggiungere Roma Capitale e, per le regioni a statuto speciale, Cagliari, Sassari, Catania, Messina e Palermo, oltre all'ente della città metropolitana del Friuli-Venezia Giulia);
   - i **comuni con popolazione superiore a 100.000 abitanti**;
   - i **comuni capoluoghi di regione**;
   - 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**;
   - le **aziende sanitarie locali**;
   - le **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;**

(di seguito "**Attori Pubblici**")

2. agli **operatori soggetti all'applicazione della normativa in materia di Perimetro di Sicurezza Nazionale Cibernetica** (PSNC) (di seguito "**Soggetti PSNC**");
3. agli **operatori sottoposti all'applicazione della Direttiva NIS** (di seguito "**Soggetti NIS**");
4. agli **operatori che forniscono reti pubbliche di comunicazioni o servizi di comunicazione elettronica accessibili al pubblico** (di seguito "**Soggetti Tel.Co.**").

## 2. ADEMPIMENTI A CARICO DEI SOGGETTI RILEVANTI PER LA LEGGE SULLA CYBERSICUREZZA

### Attori Pubblici

#### 1. Dotarsi di una struttura per la cybersicurezza

Gli Attori Pubblici devono dotarsi di una **struttura per la cybersicurezza**, anche fra quelle già esistenti, nell'ambito delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente. Tale struttura, che può essere individuata anche in quella dell'**ufficio del responsabile per la transizione al digitale**, deve provvedere a:

a. lo sviluppo di politiche e procedure di sicurezza delle informazioni;
b. la predisposizione e l'aggiornamento di un piano per il rischio informatico;
c. l'implementazione di sistemi di analisi preventiva di rilevamento del rischio informatico;
d. la produzione e l'aggiornamento di un documento che definisca i ruoli e l'organizzazione del sistema per la sicurezza delle informazioni degli Attori Pubblici;
e. la pianificazione e l'attuazione di interventi di potenziamento delle capacità per la gestione dei rischi informatici, a partire dai piani redatti;
f. la pianificazione e l'attuazione dell'adozione delle misure previste dalle linee guida per la cybersicurezza emanate dall'Agenzia per la Cybersicurezza Nazionale (ACN);
g. il monitoraggio e la valutazione continua delle minacce alla sicurezza e delle vulnerabilità dei sistemi per il loro pronto aggiornamento;
h. la verifica che i programmi e le applicazioni informatiche e di comunicazione elettronica in uso presso gli Attori Pubblici che impieghino soluzioni crittografiche rispettino le linee guida sulla crittografia e quelle sulla conservazione delle *password* adottate dall'ACN e dall'Autorità Garante per la Protezione dei Dati Personali;
i. la verifica che le applicazioni e i programmi menzionati al precedente punto *h)* non presentino vulnerabilità note.

Infine, occorre evidenziare anche che i compiti della **struttura per la cybersicurezza possono essere esercitati**

**in forma associata** (art. 17, c. 1-*sexies* e 1-*septies*, del d. lgs. 82/2005).

Per completezza, appare fin da ora opportuno sottolineare che il **criterio di selezione degli Attori Pubblici** esplicitato nella Legge sulla Cybersicurezza sembra essere particolarmente adatto per la **futura identificazione delle pubbliche amministrazioni da includere**, attraverso il decreto di recepimento italiano, **all'interno dell'alveo di applicazione della Direttiva NIS2**. Pertanto, gli Attori Pubblici ricompresi nella Legge sulla Cybersicurezza saranno verosimilmente gli stessi che – molto presto – dovranno applicare il dettato normativo della Direttiva NIS2 e del suo decreto legislativo di recepimento nazionale.

## 2. Nominare un referente per la cybersicurezza

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**. Tale soggetto, 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*.

Il legislatore, inoltre, precisa che:

a. tale soggetto può essere individuato anche nella figura del **responsabile per la transizione al digitale**;

b. 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.

Infine, si evidenzia come anche 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).

| 3. Comunicare gli incidenti | Sanzioni |
|---|---|
| **Gli Attori Pubblici devono segnalare gli incidenti indicati nella tassonomia** di cui all'art. 1, c. 3-*bis*, del d.l. 105/2019, così come convertito con modificazioni dalla l. 133/2019 (di seguito "**Decreto PSNC**"). Tale disposizione richiama, in particolare, la tassonomia **contenuta nella Determina del Direttore generale dell'Agenzia per la Cybersicurezza Nazionale del 03 gennaio 2023**. In tale contesto, il legislatore italiano richiede di **notificare gli incidenti** utilizzando le procedure disponibili sul sito internet dell'ACN, **osservando i seguenti termini**:<br>a. **massimo 24 ore**, calcolate dal momento in cui l'Attore Pubblico sia venuto a conoscenza dell'incidente, per svolgere una **prima segnalazione**;<br>b. **massimo 72 ore**, calcolate dal momento in cui l'Attore Pubblico sia venuto a conoscenza dell'incidente, per svolgere la **notifica completa**, comunicando tutte le informazioni disponibili.<br>Anche in questo caso, si sottolinea come **le modalità e i tempi di notifica** | In caso di inosservanza di tale obbligo, l'ACN invierà una comunicazione all'Attore Pubblico, avvisandolo che il reiterato inadempimento nell'arco di 5 anni comporta l'applicazione della **sanzione amministrativa** pecuniaria da un **minimo di 25.000 euro** a un **massimo di 125.000 euro**. Tale violazione, inoltre, può anche costituire causa di **responsabilità disciplinare e amministrativo-contabile** nei confronti dei funzionari e dei dirigenti responsabili. |

| | |
|---|---|
| **di tali incidenti** abbiano come scopo "secondario", in realtà, quello di allineare i soggetti coinvolti dalla novella della Legge sulla Cybersicurezza ad alcune delle previsioni normative che – molto presto – saranno previste all'interno del decreto legislativo di recepimento a livello nazionale della **Direttiva NIS2**. | |

**Decorrenza degli obblighi di comunicazione degli incidenti**

I suddetti obblighi di notifica si **applicheranno immediatamente** e, quindi, a decorrere dalla data di entrata in vigore della Legge sulla Cybersicurezza a:

- le **pubbliche amministrazioni centrali incluse nell'elenco annuale ISTAT**;
- le **regioni e province autonome di Trento e di Bolzano**;
- le **città metropolitane**.

Mentre, i medesimi obblighi di notifica, si **applicheranno dal 180º giorno** dalla data di entrata in vigore della Legge sulla Cybersicurezza a:

- i **comuni con popolazione superiore a 100.000 abitanti**;
- i **comuni capoluoghi di regione**;
- 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**;
- le **aziende sanitarie locali**;
- le **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**.

| **4. Adottare interventi risolutivi delle vulnerabilità** | **Sanzioni** |
|---|---|
| Gli Attori Pubblici devono provvedere tempestivamente all'**adozione degli interventi risolutivi indicati dall'ACN**, nel caso in cui essa **segnali specifiche vulnerabilità** cui gli Attori Pubblici risultino potenzialmente esposti. I destinatari di tali segnalazioni devono provvedere senza ritardo – e comunque **non oltre 15 giorni** dalla ricezione della comunicazione – all'adozione di tali interventi. | In caso di mancata o ritardata adozione, l'ACN invierà una comunicazione all'Attore Pubblico inadempiente, avvisandolo che la **reiterazione di tale omissione nell'arco di 5 anni** comporta l'applicazione della **sanzione amministrativa** pecuniaria da un **minimo di 25.000 euro** a un **massimo di 125.000 euro**. Tuttavia, la sanzione può non essere applicata nel caso in cui vengano tempestivamente comunicate all'ACN le **motivate esigenze di natura tecnico-organizzativa che impediscano** |

| | |
|---|---|
| | **l'adozione** degli interventi risolutivi indicati o ne comportino il differimento oltre il termine di 15 giorni. |

## Soggetti PSNC

| **1. Variare le tempistiche dell'obbligo di notifica degli incidenti che colpiscono gli *asset* non inseriti nell'elenco dei beni ICT** | **Sanzioni** |
|---|---|
| **In relazione agli obblighi di notifica degli incidenti** disciplinati nell'art. 1, c. 3-*bis*, del Decreto Perimetro, ovvero quegli incidenti che abbiano un impatto sulle reti, sui sistemi informativi e sui servizi informatici **diversi da quelli inseriti nell'elenco dei beni ICT**, si prevede che il **Soggetto PSNC debba notificarli** non più entro 72 ore, ma **osservando i seguenti termini**:<br>a. **massimo 24 ore**, calcolate dal momento in cui il Soggetto PSNC sia venuto a conoscenza dell'incidente, per svolgere una **prima segnalazione**;<br>b. **massimo 72 ore**, calcolate dal momento in cui il Soggetto PSNC sia venuto a conoscenza dell'incidente, per svolgere la **notifica completa**, comunicando tutte le informazioni disponibili.<br>Si può fin da ora sottolineare come **le modalità e i tempi di notifica di tali incidenti** abbiano come scopo "secondario", in realtà, quello di allineare i soggetti coinvolti dalla novella della Legge sulla Cybersicurezza ad alcune delle previsioni normative che – molto presto – saranno previste all'interno del decreto legislativo di recepimento a livello nazionale della **Direttiva NIS2**. | Nei casi di reiterata **inosservanza dell'obbligo di notifica**, si applica la **sanzione amministrativa pecuniaria da euro 25.000 a euro 125.000**. |

| **2. Verificare che i programmi e le applicazioni informatiche rispettino le linee guida sulla crittografia** |
|---|
| I Soggetti PSNC devono **verificare** che i programmi e le applicazioni informatiche e di comunicazione elettronica in uso che impieghino soluzioni crittografiche **rispettino le linee guida sulla crittografia e quelle sulla conservazione delle *password*** adottate dall'ACN e dall'Autorità Garante per la Protezione dei Dati Personali. Per di più, al fine di non rendere disponibili e intellegibili a terzi i dati cifrati, tali soggetti devono anche **verificare** che le applicazioni e i programmi poc'anzi menzionati **non contengano vulnerabilità note**.<br>Ciò posto, tuttavia, occorre sottolineare come la Legge sulla Cybersicurezza purtroppo **non identifichi chiaramente quale sia la struttura dei Soggetti PSNC obbligata a svolgere tale adempimento** (come avviene, invece, in maniera precisa per gli Attori Pubblici). Tuttavia, è possibile immaginare che tale responsabilità ricada sulla figura dell'**incaricato dell'attuazione del PSNC e sull'articolazione per l'implementazione del PSNC**, di cui alla Controllo ID.AM-6 del DPCM 81/2021. |

| 3. Adottare interventi risolutivi delle vulnerabilità | Sanzioni |
|---|---|
| I Soggetti PSNC devono provvedere tempestivamente all'**adozione degli interventi risolutivi indicati dall'ACN**, nel caso in cui essa **segnali specifiche vulnerabilità** cui tali soggetti risultino potenzialmente esposti. Per l'adempimento di tale obbligo, il legislatore richiede di provvedere senza ritardo e comunque **non oltre 15 giorni** dalla ricezione della comunicazione.<br><br>Anche in questo caso, purtroppo, non si può trascurare come la Legge sulla Cybersicurezza **non identifichi chiaramente quale sia la struttura obbligata a svolgere tale adempimento** (come avviene invece per gli Attori Pubblici). Tuttavia, è possibile immaginare che tale responsabilità ricada sulla figura dell'**incaricato dell'attuazione del PSNC e sull'articolazione per l'implementazione del PSNC**, di cui al Controllo ID.AM-6 del DPCM 81/2021. | In caso di mancata o ritardata adozione degli interventi risolutivi indicati, l'ACN invierà una comunicazione a tali soggetti, avvisandoli che la **reiterazione di tale omissione nell'arco di 5 anni** comporterà l'applicazione della **sanzione amministrativa** pecuniaria da un **minimo di 25.000 euro** a un **massimo di 125.000 euro**. Ciò, a meno che non vengano tempestivamente comunicate all'ACN **le motivate esigenze di natura tecnico-organizzativa che impediscano l'adozione** degli interventi risolutivi indicati o che comportino il differimento oltre il termine di 15 giorni. |

## Soggetti NIS

### 1. Verificare che i programmi e le applicazioni informatiche rispettino le linee guida sulla crittografia

I Soggetti NIS **verificano** che i programmi e le applicazioni informatiche e di comunicazione elettronica in uso che impieghino soluzioni crittografiche **rispettino le linee guida sulla crittografia e quelle sulla conservazione delle *password*** adottate dall'ACN e dall'Autorità Garante per la Protezione dei Dati Personali. Per di più, al fine di non rendere disponibili e intellegibili a terzi i dati cifrati, tali soggetti devono anche **verificare** che le applicazioni e i programmi poc'anzi menzionati **non contengano vulnerabilità note**.

Ciò posto, tuttavia, occorre sottolineare come la Legge sulla Cybersicurezza purtroppo **non identifichi chiaramente quale sia la struttura del Soggetto NIS obbligata a svolgere tale adempimento.** Ad ogni modo, su tale tema non è possibile scendere nei dettagli in questa sede, in quanto le "*Linee guida per l'adozione delle misure di sicurezza da parte degli OSE e per la notifica degli incidenti*" sono tuttora da considerarsi come "*Informazioni non Classificate Controllate*".

| 2. Adottare interventi risolutivi delle vulnerabilità | Sanzioni |
|---|---|
| I Soggetti NIS devono provvedere tempestivamente all'**adozione degli interventi risolutivi indicati dall'ACN**, nel caso in cui essa **segnali** | In caso di mancata o ritardata adozione degli interventi risolutivi |

| | |
|---|---|
| **specifiche vulnerabilità** cui tali soggetti risultino potenzialmente esposti. Per l'adempimento di tale obbligo, il legislatore richiede di provvedere senza ritardo e comunque **non oltre 15 giorni** dalla ricezione della comunicazione.<br><br>Ciò posto, tuttavia, occorre sottolineare come la Legge sulla Cybersicurezza purtroppo **non identifichi chiaramente quale sia la struttura del Soggetto NIS obbligata a svolgere tale adempimento.** Ad ogni modo, su tale ultimo tema, non è possibile scendere nei dettagli in questa sede, in quanto le "*Linee guida per l'adozione delle misure di sicurezza da parte degli OSE e per la notifica degli incidenti*" sono tuttora da considerarsi come "*Informazioni non Classificate Controllate*". | indicati, l'ACN invierà una comunicazione a tali soggetti, avvisandoli che la **reiterazione di tale omissione nell'arco di 5 anni** comporterà l'applicazione della **sanzione amministrativa** pecuniaria da un **minimo di 25.000 euro** a un **massimo di 125.000 euro**. Ciò, a meno che non vengano tempestivamente comunicate all'ACN **le motivate esigenze di natura tecnico-organizzativa che impediscano l'adozione** degli interventi risolutivi indicati o che comportino il differimento oltre il termine di 15 giorni. |

| **Soggetti Tel.Co.** | |
|---|---|
| **1. Adottare interventi risolutivi delle vulnerabilità** | **Sanzioni** |
| I Soggetti Tel.Co., ovvero le **imprese che forniscono reti pubbliche di comunicazioni** o **servizi di comunicazione elettronica** accessibili al pubblico, devono provvedere tempestivamente all'**adozione degli interventi risolutivi indicati dall'ACN**, nel caso in cui essa **segnali specifiche vulnerabilità** cui tali soggetti risultino potenzialmente esposti. Per l'adempimento di tale obbligo, il legislatore richiede di provvedere senza ritardo e comunque **non oltre 15 giorni** dalla ricezione della comunicazione.<br><br>Anche in questo caso, purtroppo, non si può trascurare come la Legge sulla Cybersicurezza **non identifichi chiaramente per i Soggetti Tel.Co. quale sia la struttura obbligata a svolgere tale adempimento.** | In caso di mancata o ritardata adozione degli interventi risolutivi indicati, l'ACN invierà una comunicazione a tali soggetti, avvisandoli che la **reiterazione di tale omissione nell'arco di 5 anni** comporterà l'applicazione della **sanzione amministrativa** pecuniaria da un **minimo di 25.000 euro** a un **massimo di 125.000 euro**. Ciò, a meno che non vengano tempestivamente comunicate all'ACN **le motivate esigenze di natura tecnico-organizzativa che impediscano l'adozione** degli interventi risolutivi indicati o che comportino il differimento oltre il termine di 15 giorni. |

## 3. MODIFICHE ALLA NORMATIVA IN MATERIA DI RESPONSABILITÀ AMMINISTRATIVA DEGLI ENTI *EX* D.LGS. 231/2001

La Legge sulla Cybersicurezza interviene anche sul catalogo dei **reati presupposto** in materia di responsabilità amministrativa degli enti di cui al d. lgs. 231/2001. In particolare, il legislatore:

1. modifica il contenuto dell'**art. 24-*bis* relativo ai reati informatici**, aumentando le sanzioni previste all'interno del suo c. 1, le quali passano da una cornice edittale ricompresa tra cento e cinquecento quote, ad una ricompresa tra **duecento e settecento quote**;

2. aggiunge all'art. 24-*bis* il **nuovo c. 1-*bis***, ai sensi del quale si applica all'ente la **sanzione pecuniaria da trecento a ottocento quote** in relazione alla commissione della **nuova fattispecie di reato** – introdotta sempre dalla Legge sulla Cybersicurezza – **legata all'estorsione informatica** di cui all'art. 629, c. 3, c.p.. Nei casi di condanna, inoltre, è prevista anche l'applicazione **delle sanzioni interdittive** previste dall'art. 9, c. 2, del d. lgs. 231/2001, per una durata non inferiore a due anni;

3. modifica il c. 2 dell'art. 24-*bis*, relativo alla commissione dei delitti di cui agli artt. 615-*quater* ("*Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici e telematici*") e 615-*quinquies* ("*Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico*") c.p., **innalzando la sanzione pecuniaria ivi prevista sino a quattrocento quote**;

4. sostituisce tra i reati presupposto per i quali è prevista l'applicazione all'ente della sanzione pecuniaria di cui al precedente punto (3.) il riferimento all'art. 615-*quinquies* c.p., abrogato proprio dalla Legge sulla Cybersicurezza, con il richiamo al **nuovo delitto di detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico di cui all'art. 635-*quater*.1**.

## 4. PRINCIPALI NOVITÀ DA SEGUIRE IN MATERIA DI CONTRATTI PUBBLICI DI BENI E SERVIZI INFORMATICI IMPIEGATI IN UN CONTESTO CONNESSO ALLA TUTELA DEGLI INTERESSI NAZIONALI STRATEGICI

La Legge sulla Cybersicurezza introduce nella disciplina dei **contratti pubblici di beni e servizi informatici** alcuni **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.

Tali **elementi essenziali di cybersicurezza** saranno individuati da uno specifico Decreto del Presidente del Consiglio dei Ministri da **emanarsi entro 120 giorni** dall'entrata in vigore della Legge sulla Cybersicurezza. Tale Decreto del Presidente del Consiglio dei Ministri, peraltro, provvederà anche a dettagliare i casi in cui, per la tutela della sicurezza nazionale, debbano essere previsti **criteri di**

**premialità per le proposte o le offerte che contemplino l'uso di tecnologie di cybersicurezza italiane** o di Paesi appartenenti all'**Unione europea** o di Paesi aderenti all'Alleanza atlantica (**NATO**) o di **Paesi terzi** – individuati nel medesimo decreto – tra quelli che hanno **accordi di collaborazione con l'Unione europea o con la NATO in materia di cybersicurezza, protezione delle informazioni classificate, ricerca e innovazione**.

Ciò posto, i soggetti che saranno tenuti a rispettare quanto previsto in questo ambito dalla Legge sulla Cybersicurezza sono:

- le **pubbliche amministrazioni**, comprese le autorità di sistema portuale e le autorità amministrative indipendenti di garanzia, vigilanza e regolazione;
- i **gestori di servizi pubblici**, ivi comprese le società quotate in relazione ai servizi di pubblico interesse;
- le **società a controllo pubblico**, escluse le società quotate a meno che non gestiscano servizi di pubblico interesse;
- i **soggetti privati** rientranti nel **Perimetro di Sicurezza Nazionale Cibernetica**.

Inoltre, nell'ambito dei **contratti di approvvigionamento di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici** e sempre in relazione agli **elementi essenziali di cybersicurezza**, vengono previsti per le **stazioni appaltanti**, ivi incluse le **centrali di committenza**, i seguenti **obblighi e facoltà**:

- esercitare le **facoltà di cui agli artt. 107, c. 2, e 108, c, 10, del d. lgs. 36/2023** (di seguito "**Codice dei contratti pubblici**"), qualora accertino che l'offerta **non tiene conto degli elementi essenziali di cybersicurezza** individuati nel futuro Decreto del Presidente del Consiglio dei Ministri;
- **considerare sempre gli elementi essenziali di cybersicurezza** nella valutazione dell'**elemento qualitativo**, ai fini dell'individuazione del miglior rapporto qualità/prezzo per l'aggiudicazione;
- inserire gli **elementi di cybersicurezza tra i requisiti minimi dell'offerta** nel caso in cui sia utilizzato il **criterio del minor prezzo**, ai sensi dell'art. 108, c. 3, del Codice dei contratti pubblici;
- stabilire un **tetto massimo per il punteggio economico entro il limite del 10%** nel caso in cui sia utilizzato il **criterio dell'offerta economicamente più vantaggiosa (OEPV)**, ai sensi dell'art. 108, c. 4, del Codice dei contratti pubblici, nella valutazione dell'**elemento qualitativo** ai fini dell'individuazione del migliore rapporto qualità/prezzo;
- prevedere – nei casi individuati nel futuro Decreto del Presidente del Consiglio dei Ministri – **criteri di premialità** per le proposte o le offerte che contemplino l'uso di **tecnologie di cybersicurezza italiane** o di Paesi appartenenti all'**Unione europea** o di Paesi aderenti all'Alleanza atlantica (**NATO**) o di **Paesi terzi** tra quelli che hanno **accordi di collaborazione con l'Unione europea o con la NATO in materia di cybersicurezza, protezione delle informazioni classificate, ricerca e innovazione**. Ciò, al fine di tutelare la sicurezza nazionale e di conseguire l'autonomia tecnologica e strategica dell'Italia nell'ambito della cybersicurezza.

## 5. PRECLUSIONI IN RELAZIONE ALL'ASSUNZIONE DI PERSONALE CHE ABBIA RICOPERTO SPECIFICI RUOLI PRESSO ALCUNE PUBBLICHE AMMINISTRAZIONI CENTRALI

La Legge sulla Cybersicurezza introduce alcune **preclusioni all'assunzione** di personale che abbia ricoperto specifici ruoli presso alcune **pubbliche amministrazioni centrali**.

In particolare, si prevede che i dipendenti appartenenti al ruolo del personale dell'**ACN** che abbiano partecipato, nell'interesse e a spese della stessa, a **specifici percorsi formativi di specializzazione**, non possano essere assunti, né assumere incarichi presso soggetti privati per **mansioni legate alla materia della cybersicurezza** per i **due anni** successivi a decorrere dalla data di completamento dell'ultimo di tali percorsi formativi.

Peraltro, i **contratti stipulati** in violazione di quanto disposto dalla Legge sulla Cybersicurezza **sono nulli**.

Per il "*mondo dell'intelligence*", invece, la Legge sulla Cybersicurezza prevede una preclusione per coloro che abbiano ricoperto:

- la carica di **direttore generale** o di **vice direttore generale del Dipartimento delle Informazioni per la Sicurezza (DIS)**;
- la carica di **direttore** o di **vice direttore dell'Agenzia informazioni e sicurezza esterna (AISE)**;
- la carica di **direttore** o di **vice direttore dell'Agenzia informazioni e sicurezza interna (AISI)**;
- incarichi **dirigenziali di prima fascia di preposizione a strutture organizzative di livello dirigenziale generale**.

La Legge sulla Cybersicurezza prevede che tali soggetti, nei **tre anni successivi alla cessazione dall'incarico**, non possano svolgere **attività lavorativa professionale o di consulenza**, né ricoprire **cariche presso soggetti esteri, pubblici o privati**, ovvero presso **soggetti privati italiani che svolgano attività di rilevanza strategica**, secondo la perimetrazione tracciata dal d.l. 21/2012.

Per di più, viene aggiunto anche un **divieto inderogabile** per il personale appartenente al **ruolo unico del personale dei Servizi di Informazione per la Sicurezza e del Dipartimento delle Informazioni per la Sicurezza** di svolgere, nei **tre anni successivi alla cessazione del loro servizio**, attività lavorativa, professionale o consulenziale, così come di ricoprire cariche, presso **enti o privati titolari di licenza per prestare vigilanza o custodia**, ovvero in ogni caso nei confronti di soggetti che a qualunque titolo svolgano **attività di investigazione, ricerca o raccolta informativa**.

Un medesimo **divieto inderogabile**, infine, viene prescritto per il personale appartenente al **ruolo unico del personale dei servizi di informazione per la sicurezza e del Dipartimento delle Informazioni per la Sicurezza**, qualora abbia partecipato a specifici **percorsi formativi di specializzazione** nell'interesse e a spese del DIS, dell'AISE e dell'AISI. In particolare, il legislatore prevede un divieto di assunzione o di assunzione di **incarichi presso soggetti privati, per svolgere le mansioni per le quali abbia beneficiato delle attività formative**. Anche in questo caso, il divieto ha la durata di **tre anni** a decorrere dalla data di **completamento dell'ultimo dei percorsi formativi**.

In tutti i casi finora analizzati, i **contratti stipulati e gli incarichi conferiti** in violazione dei divieti **sono nulli**.

Pertanto, qualora le pubbliche amministrazioni o i soggetti privati abbiano intenzione di assumere personale proveniente dalle summenzionate pubbliche amministrazioni centrali, **appare opportuno accertare anche che non operi nessuna delle preclusioni sopra individuate**.

## 6. PROSSIME AZIONI

Dall'analisi del nuovo quadro normativo risulta già chiara la mole di **nuovi adempimenti ai quali sia le pubbliche amministrazioni che i soggetti privati dovranno adeguarsi**.

Pertanto, si ritiene necessario procedere quanto prima alla predisposizione di un piano di adeguamento, che consenta di determinare l'effettivo impatto sull'organizzazione della Legge sulla Cybersicurezza.

In particolare, si ritiene che **la sfida più complessa** sia proprio quella di **valutare gli adempimenti già svolti ai sensi delle normative emanate nell'ambito della cybersicurezza** (*i.e.*, Direttiva NIS, PSNC, Decreto Telco) e, in un'ottica di efficienza operativa sul piano tecnico, legale e dei processi interni, **comprendere i punti di intersezione e raccordo**.



**Stefano Mele**
**Partner**
Responsabile Cybersecurity & Space Economy Law
co-Responsabile Privacy Law
Roma
+39 06 478751
smele@gop.it