

# Messaggio

| numero      | data            | Dipartimento                      |
|-------------|-----------------|-----------------------------------|
| <b>7488</b> | 17 gennaio 2018 | FINANZE ED ECONOMIA / CANCELLERIA |
| Concerne    |                 |                                   |

## **Modifica della Legge sull'ordinamento degli impiegati dello Stato e dei docenti del 15 marzo 1995 (LORD) riguardante la protezione dei dati personali**

Signor Presidente,  
signore e signori deputati,

con il presente messaggio sottoponiamo alla vostra attenzione un progetto di modifica della Legge sull'ordinamento degli impiegati dello Stato e dei docenti del 15 marzo 1995 (LORD) vertente a disciplinare la protezione dei dati personali.

### **I. INTRODUZIONE**

La corretta ed efficace gestione del personale pubblico presuppone l'elaborazione di un numero considerevole di dati personali. L'allegato 1 dell'Ordinanza sulla protezione dei dati personali del personale federale del 26 ottobre 2011<sup>1</sup> mostra la quantità e la qualità di categorie di dati personali che possono essere elaborate nel settore lavorativo pubblico. A livello cantonale, la situazione non è diversa.

I Servizi centrali del personale – cui appartengono la Sezione delle risorse umane, la Sezione amministrativa del Dipartimento dell'educazione, della cultura e dello sport (DECS) e la Direzione dell'Istituto delle assicurazioni sociali – nonché, attualmente, la Sezione delle scuole comunali del DECS per i docenti delle scuole comunali necessitano, in qualità di organi responsabili dell'elaborazione dei dati dei dipendenti pubblici, informazioni a carattere personale riguardanti i dipendenti sottoposti alla LORD per adempiere ai loro compiti legali di gestione del personale. L'elaborazione di dati è quindi di principio giustificata dall'interesse pubblico alla gestione amministrativa e legale dei dipendenti pubblici.

Tuttavia, quando l'elaborazione di dati è sistematica – vale a dire regolare e duratura (e, di norma, effettuata tramite l'ausilio di una banca dati) – e concerne anche dati meritevoli di particolare protezione, com'è il caso nel settore lavorativo pubblico, la Legge sulla protezione dei dati personali del 9 marzo 1987<sup>2</sup> prevede l'obbligo di legiferare a livello formale (art. 6 cpv. 1 LPDP). Ciò significa che, oltre a riconoscere e recepire nel diritto l'interesse pubblico in questione, il Legislatore è chiamato a definire le elaborazioni di dati che ne conseguono, prevedendo in particolare gli scopi e le condizioni delle stesse. Così, la base legale deve indicare perlomeno lo scopo dell'elaborazione, l'organo responsabile, l'oggetto, le modalità di elaborazione, nonché la norma di delega al Consiglio di Stato per la regolamentazione esecutiva. L'obbligo della base legale è previsto anche per la procedura di richiamo (art. 14 cpv. 3 LPDP).

<sup>1</sup> OPDPers; RS 172.220.111.4

<sup>2</sup> LPDP; RL 1.6.1.1

Lo scopo della base legale per le elaborazioni e trasmissioni sistematiche di dati consiste principalmente nel garantire la sicurezza del diritto e contribuire alla tutela dei diritti fondamentali, in particolare della personalità e della sfera privata delle persone i cui dati sono elaborati. Attualmente, la LORD enuncia il principio generale della protezione della personalità (art. 1c cpv. 2 lett. g) LORD), nonché il divieto di divulgare gli affari di servizio (segreto d'ufficio, art. 29 LORD). Prevede, inoltre, l'obbligo dello Stato di consultare le organizzazioni del personale prima di creare o modificare sistemi per il trattamento di dati (art. 1d cpv. 2 lett. b) LORD). Infine, all'art. 52a, intitolato protezione della sfera personale, disciplina il rispetto della dignità e dell'integrità fisica e psichica dell'impiegato, segnatamente in materia di molestie psicologiche e sessuali, tuttavia senza riferimento alla protezione dei dati. Un adattamento alle esigenze normative della LPDP è dunque inevitabile. Le nuove norme elaborate sono affiancate dalla LPDP quale normativa generale e complementare.

La cerchia delle persone interessate dalla presente revisione sono i dipendenti pubblici secondo l'art. 1 cpv. 1 lett. a) e b) LORD. Coprendo quindi anche i docenti cantonali e comunali, le attuali norme della Legge della scuola del 1° febbraio 1990<sup>3</sup> (art. 91a segg.) – limitatamente all'elaborazione dei dati personali di questa categoria di dipendenti pubblici – sono abrogate e sostituite dalle nuove normative, unificando quindi le disposizioni sull'elaborazione di dati di tutti i dipendenti soggetti alla LORD.

## **II. I SISTEMI D'INFORMAZIONE DEI SERVIZI CENTRALI DEL PERSONALE**

I Servizi centrali del personale e la Sezione delle scuole comunali del DECS fanno capo a sistemi d'informazione elettronici per l'elaborazione sistematica di dati relativi al rapporto d'impiego, dalla loro raccolta – al momento della candidatura o durante il rapporto di lavoro – alla loro conservazione, archiviazione o distruzione. I dati sovengono alle necessità amministrative, organizzative e legali del rapporto d'impiego. Gli organi responsabili gestiscono in tal senso archivi di dati (banche dati) e documentali finalizzati alla selezione del personale, alla gestione amministrativa, organizzativa, salariale e del contenzioso dei dipendenti. Tali sistemi d'informazione possono contenere dati meritevoli di particolare protezione, segnatamente in relazione alla situazione familiare del dipendente oppure a procedimenti disciplinari o penali.

La revisione fissa nella LORD queste elaborazioni sistematiche di dati, compresa la gestione delle candidature, per le quali è istituito lo standard di presentazione in forma digitale, e dei dossier del personale in forma elettronica. Agli organi responsabili, così come ai singoli dipartimenti o unità amministrative, è inoltre garantita la facoltà di eseguire ulteriori e puntuali elaborazioni (in particolare, trasmissioni) di dati del personale in garanzia d'interessi legittimi del personale o dell'Amministrazione pubblica. I commenti ai singoli articoli chiariscono questa facoltà con degli esempi concreti.

## **III. LA PROCEDURA DI RICHIAMO**

La procedura di richiamo permette agli utenti autorizzati di accedere direttamente ai dati presenti nei sistemi d'informazione dei Servizi centrali del personale e della Sezione delle scuole comunali del DECS, senza passare per il loro tramite e filtro, e di svolgere così più rapidamente ed efficacemente i propri compiti legali. L'accesso diretto a archivi di dati deve poggiare su una base legale formale, nel caso in cui siano dati personali degni di particolare protezione o profili della personalità ad essere elaborati (art. 6 e 14 cpv. 3 LPDP combinati).

---

<sup>3</sup> LSc; RL 5.1.1.1.

L'utente (ad esempio, il funzionario dirigente autorizzato) che richiede l'informazione decide il momento, il modo e l'estensione dell'accesso nel caso specifico, e ciò senza che il Servizio centrale in questione – quale organo responsabile dei dati secondo l'art. 4 cpv. 6 LPDP – esamini, ad ogni singola richiesta, la liceità, l'estensione e la motivazione della consultazione. La procedura di richiamo permette di accedere ripetutamente agli stessi dati su un arco di tempo indefinito.

L'attribuzione degli accessi a tali sistemi è preceduta da una richiesta scritta e motivata da parte del richiedente. L'autorizzazione è data all'interessato dal Servizio centrale, rispettivamente dalla Sezione delle scuole comunali del DECS, successivamente alla constatazione di fondatezza e necessità dell'accesso tramite procedura di richiamo. L'accesso è modulato in funzione delle reali necessità informative dell'utente, che il Servizio centrale valuta e definisce preventivamente all'autorizzazione di accesso.

#### **IV. LA TRASMISSIONE DI DATI IN SINGOLI CASI**

La trasmissione di dati personali quale forma particolare di elaborazione di dati, la cui tipologia più importante è la procedura di richiamo, è la fase più delicata dal punto di vista della protezione dei dati. Anche la trasmissione in singoli casi – seppur con modalità e frequenza diverse da quella sistematica (procedura di richiamo) – può presentare, a seconda delle circostanze concrete del caso, un potenziale di rischio per la personalità delle persone interessate. A differenza della procedura di richiamo, che può essere giustificata unicamente da una base legale, la trasmissione in singoli casi può esserlo anche dalla necessità di disporre di dati personali per l'adempimento di un compito legale o dal consenso della persona interessata.

La trasmissione nel singolo caso è un concetto non chiaramente definito da dottrina e giurisprudenza in tutti i suoi elementi costitutivi, per cui è importante fornire qui di seguito possibili elementi di definizione del concetto. Sulla base di questi elementi i Servizi centrali del personale e la Sezione delle scuole comunali del DECS possono riconoscere il tipo di trasmissione e le condizioni cui essa è soggetta.

Sono in generale riconosciuti i seguenti elementi cumulativi costitutivi dell'elaborazione di dati in singoli casi: l'unicità (o specificità) dello scopo e la singolarità temporale dell'elaborazione, vale a dire la sua limitazione nel tempo (assenza di carattere permanente, regolare o duraturo dell'elaborazione). L'elaborazione di dati in singoli casi presuppone inoltre la ponderazione degli interessi in gioco da parte dell'organo responsabile dei dati a ogni richiesta di dati, la determinazione (cioè la chiara definizione e delimitazione) delle persone interessate e la forma qualificata della richiesta dei dati personali, che deve essere scritta e motivata<sup>4</sup>.

L'elaborazione nel singolo caso non è quindi data quando avviene per il tramite di una procedura di richiamo, già per il solo motivo che quest'ultima implica regolarità e durata e un'unica ponderazione degli interessi da parte del legislatore prima della promulgazione della rispettiva base legale – dunque non a ogni singola elaborazione.

#### **V. L'ELABORAZIONE DI DATI RELATIVI ALLA SALUTE**

Il Servizio medico del personale dell'Amministrazione cantonale gestisce i dati medici relativi al personale assunto e ai candidati ai concorsi pubblici. Il compito pubblico alla base dell'elaborazione dei dati medici consiste nella valutazione dello stato di salute rispettivamente della capacità lavorativa del dipendente rispettivamente candidato. Poiché

---

<sup>4</sup> Rapporto n. 7061R del 2 settembre 2015 della Commissione della legislazione sul messaggio 18 marzo 2015 concernente la modifica della Legge sulla protezione dei dati personali del 9 marzo 1987 (LPDP) riguardante i motivi giustificativi e i principi che reggono l'elaborazione di dati personali (art. 6 e 7 LPDP), pag. 9 segg.

i dati sulla salute sono meritevoli di particolare protezione (art. 4 cpv. 2 LPDP), la loro elaborazione sistematica presuppone una base legale in senso formale nel diritto settoriale, conformemente all'art. 6 cpv. 1 LPDP. Il personale del Servizio medico è soggetto al segreto professionale<sup>5</sup> e al segreto d'ufficio<sup>6</sup> ed è funzionalmente e strutturalmente separato dalla Sezione delle risorse umane, alla quale rimane allacciato amministrativamente. La proposta di normativa viene a colmare la lacuna concernente le basi legali per l'elaborazione sistematica di dati sulla salute dei dipendenti pubblici.

I medici di fiducia dell'Istituto delle assicurazioni sociali (IAS) e dei comuni per quanto riguarda gli impiegati di tale Istituto, rispettivamente i docenti comunali, sono mandatari dello stesso compito pubblico del Servizio medico del personale dell'Amministrazione cantonale. In quanto mandatari di compiti pubblici, essi sono parificati, per quanto riguarda la protezione dei dati, a organi cantonali, rispettivamente comunali, ai sensi dell'art. 2 LPDP. Tuttavia, essi non sono soggetti alla LORD. A loro si applicano esclusivamente i precetti generali della LPDP e il segreto medico previsto dal Codice penale.

## **VI. LA SORVEGLIANZA SUL POSTO DI LAVORO**

La sorveglianza è una misura delicata, sia sul piano giuridico sia su quello umano e sociale. Per essere lecita, deve seguire precise e restrittive regole e condizioni. Nel settore lavorativo, la sorveglianza può essere definita come misura di controllo prolungato e in tempo reale del rispetto delle norme comportamentali da parte del dipendente, in particolare riguardanti l'uso delle risorse informatiche. La sorveglianza si distingue dall'analisi puntuale delle tracce relative all'uso delle risorse informatiche, cioè quella misura di controllo circoscritta ad un momento determinato e limitato nel tempo. La sorveglianza nominativa prolungata o duratura è proibita dal diritto federale sul lavoro, mentre l'analisi nominativa puntuale delle tracce relative all'uso dei sistemi informativi è lecita, a determinate condizioni<sup>7</sup>.

La sorveglianza in quanto misura con componente temporale qualificata può quindi aver luogo unicamente in maniera non nominativa e ha come oggetto il comportamento dell'insieme dei dipendenti di una determinata unità amministrativa. Se, in quell'ambito, è riscontrato un comportamento contrario alle regole stabilite dal datore di lavoro, quest'ultimo (e, per esso, i servizi abilitati) può procedere a un'ulteriore analisi delle stesse tracce in modo pseudonimo, vale a dire mirato su determinate categorie di dati (ad esempio, l'indirizzo IP di computer) riconducibili a persone identificabili. Se l'analisi pseudonima delle tracce conferma la ripartizione degli abusi sull'insieme dei dipendenti dell'unità amministrativa, senza preponderanza degli stessi su singoli dipendenti, il datore di lavoro si limita di principio a richiamare tutti i dipendenti al rispetto delle direttive vigenti in materia di uso delle risorse informatiche, senza identificare singole persone. Se, invece, gli abusi si concentrano su singoli indirizzi IP, il datore di lavoro può procedere all'identificazione (comparazione degli indirizzi IP in questione con una lista nominativa di corrispondenza) e sanzionamento dei responsabili.

Ciò è, in sintesi, la conclusione cui giunge la Guida dell'Incaricato federale della protezione dei dati e della trasparenza (IFPDT) sulla Sorveglianza dell'utilizzazione di Internet e della posta elettronica sul posto di lavoro. In una pubblicazione in RtiD I-2013 dal titolo "La sorveglianza sul posto di lavoro: occorrono nuove basi legali", si precisa che la sorveglianza finalizzata al controllo in tempo reale e prolungato dell'uso delle risorse informatiche tramite controllo automatico e sistematico delle giornalizzazioni riguardanti l'uso delle risorse informatiche non può essere tesa alla ricerca nominativa di abusi di Internet o della posta elettronica, rispettivamente alla formazione di un relativo sospetto

---

<sup>5</sup> Art. 321 CP.

<sup>6</sup> Art. 29 Legge sull'ordinamento degli impiegati dello Stato e dei docenti; LORD; RL 2.5.4.1.

<sup>7</sup> Art. 26 Ordinanza 3 concernente la legge sul lavoro; OLL 3; RS 822.113.

concreto. L'abuso può essere constatato unicamente tramite una sorveglianza non nominativa (analisi anonime o pseudonime dei logfile, ossia del registro contenente il protocollo degli eventi del sistema, quali la cronologia e l'oggetto degli accessi da parte degli utenti autorizzati) o grazie a indizi fortuiti (vedi anche DTF 8C\_448/2012 del 17 gennaio 2013, consid. 5.2, 5.5.4 e 5.5.6). L'adozione della modifica della LORD riguardante la protezione dei dati personali avrà come conseguenza un aggiornamento delle normative specifiche per i dipendenti, che dovranno confluire in un Regolamento.

Il presente pacchetto normativo prevede una norma sulla sorveglianza che riprende la dottrina e la giurisprudenza svizzere ed è conforme al diritto pubblico federale sul lavoro, in particolare all'art. 26 OLL 3.

Come già ribadito in entrata, costituendo la sorveglianza un'elaborazione sistematica di dati – vale a dire presentando la caratteristica di regolarità o durata nel tempo – e concernendo potenzialmente dati personali meritevoli di particolare protezione che possono costituire, nel loro insieme, un profilo della personalità, la base legale della sorveglianza deve essere prevista sul piano legale formale.

## **VII. COMMENTO AI SINGOLI ARTICOLI**

### **Art. 13 cpv. 1 (modificato)**

L'art. 13 definisce le modalità di presentazione del dossier di candidatura e il cpv. 1 in particolare il rimando al bando di concorso per quanto riguarda i documenti che i candidati devono produrre. Pur rimanendo vincolato al principio generale della proporzionalità, il legislatore si svincola così dalla definizione di un elenco concreto di documenti da produrre e rinvia invece al rispettivo bando di concorso nel singolo caso.

Così facendo, si tiene maggiormente conto delle concrete esigenze informative di ogni singolo concorso e in particolare dei differenti requisiti, ritenute le molteplici tipologie di funzioni nell'Amministrazione cantonale.

Nel contempo, l'articolo prevede la presentazione della documentazione da parte dei candidati di principio in forma digitale (e-candidatura).

### **Art. 13 cpv. 2 (stralciato)**

Lo stralcio del cpv. 2 (esonero dalla presentazione dei documenti per i dipendenti dello Stato) è conseguenza del rimando al bando di concorso di cui al cpv. 1. Nel contempo, si ritiene adeguato che il candidato interno motivi la sua candidatura a un posto di lavoro presso una nuova unità amministrativa.

### **Art. 31a (modificato)**

Per chiarezza, si modifica il passaggio “[...] **esso** è tenuto a trasmettere immediatamente la segnalazione al Ministero pubblico” con “[...] **quest'ultimo** è tenuto a trasmettere immediatamente la segnalazione al Ministero pubblico”, facendo così univocamente riferimento al Consiglio di Stato e non al dipendente.

## **TITOLO IV – Protezione dei dati**

I nuovi articoli inerenti alla protezione dei dati dei dipendenti e dei sistemi d'informazione legati alla gestione del personale e degli stipendi sono inseriti al Titolo IV (art. 84 e 84a-i), con la nuova dicitura “Protezione dei dati”.

## **Art. 84 (nuovo)**

Il cpv. 1 della norma definisce gli organi responsabili dell'elaborazione dei dati dei dipendenti pubblici e gli scopi dei sistemi informativi. I Servizi centrali del personale e la Sezione delle scuole comunali del DECS (in particolare quest'ultimo per la gestione degli stipendi e della carriera salariale dei docenti comunali) assumono così il dovere legale di una gestione delle informazioni a carattere personale conforme alla legislazione sulla protezione della personalità e al diritto in generale (principio della liceità). Essi sono in particolare legittimati a elaborare dati personali, tuttavia limitatamente ai dati strettamente necessari per l'adempimento dei loro compiti legali (principi della proporzionalità e della finalità). La norma precisa che l'elaborazione dei dati del personale avviene per il tramite di sistemi elettronici d'informazione e di documentazione – di cui i principali sono SAP e, per la gestione amministrativa dei docenti, GAS cantonale e comunale – e i cui scopi sono definiti e delimitati espressamente, ovvero:

- gestione elettronica delle candidature (lett. a) e degli incarti del personale (lett. b);
- gestione amministrativa del personale, dell'organizzazione, dei salari e delle assenze e presenze (lett. b);
- allestimento di statistiche (lett. c).

Al cpv. 2 si precisa che ogni Servizio centrale accede ai dati necessari ad adempiere ai propri compiti; ad es. l'Ufficio degli stipendi e delle assicurazioni accede ai dati inerenti alle ore effettivamente prestate dai docenti contenute in GAS per il calcolo del loro salario in SAP.

Il cpv. 3 prevede le principali categorie di dati personali elaborati:

- dati anagrafici, sulla formazione e sull'esperienza professionale e sullo stato familiare e della salute;
- dati riguardanti le varie tappe e eventi del rapporto lavorativo, dal concorso di assunzione, alla carriera professionale, all'uscita;
- dati amministrativi riguardanti le presenze/assenze;
- dati inerenti alle procedure amministrative o disciplinari;
- dati necessari al calcolo e al versamento del salario e delle indennità;
- tutti i documenti rilevanti per il rapporto d'impiego, dalla candidatura alla conclusione dello stesso.

Più specificatamente, in ossequio al principio della legalità e dei corollari principi di adeguatezza della densità e del livello normativo, il cpv. 3 prevede la facoltà dei servizi competenti di elaborare dati meritevoli di particolare protezione in relazione alla sfera familiare, alle valutazioni sulle prestazioni e sul comportamento professionali nonché a procedimenti amministrativi, disciplinari o penali.

Per quanto riguarda i dati sulla salute, i servizi di cui al cpv. 1 gestiscono unicamente informazioni generiche originate dalle timbrature relative alle presenze/assenze per malattia, nonché le risultanze generiche fornite dal Servizio medico del personale.

Il cpv. 4 prevede che il Centro sistemi informativi (CSI) e il Servizio d'informatica dell'Istituto delle assicurazioni sociali garantiscono il buon funzionamento e la sicurezza dell'infrastruttura tecnica e degli applicativi e la loro manutenzione.

## **Art. 84a (nuovo)**

Il nuovo articolo prevede la digitalizzazione di documenti cartacei, in particolare dei dossier dei dipendenti. Partendo dal documento cartaceo, originale o in copia, e con l'ausilio di specifiche tecnologie (ad esempio, la firma digitale), è creata una copia digitale identica, o equivalente, del documento cartaceo, tramite digitalizzazione, o scansione, dello stesso. È così garantita l'integrità della copia. Poiché identico, il documento elettronico può quindi espletare gli stessi effetti giuridici del documento cartaceo, in particolare presentare lo stesso valore probatorio. Quanto all'ammissibilità in giudizio di documenti elettronici, in caso di contenzioso di natura civile, secondo gli articoli 177-180 del Codice di procedura civile (CPC) gli *"atti in forma elettronica vanno ammessi come prove alla stessa stregua dei supporti di dati tradizionali"* e ancora *"è irrilevante che si tratti sin dall'inizio di atti in forma elettronica o di documenti sottoposti a scansione soltanto in un secondo tempo"*. Si crea così un documento elettronico presunto equivalente a quello cartaceo.

Come per il documento cartaceo, anche per la sua copia elettronica la presunzione di autenticità può però essere contestata. Il documento cartaceo può, infatti, essere stato manipolato o falsificato prima della sua digitalizzazione. In una simile ipotesi, la copia elettronica rappresenta unicamente una copia identica, o equivalente, di un documento cartaceo precedentemente modificato. In caso di contestazione dell'autenticità di un documento elettronico, il CPC evidenzia che *"La controparte non può tuttavia limitarsi ad asserire che quest'ultimo [documento scansionato] non è autentico; deve anzi addurre elementi concreti atti a suscitare nel giudice seri dubbi circa l'autenticità del contenuto del documento o della firma che esso reca"*, cosicché si lascia concludere che *"finché non sia dimostrato il contrario, questi supporti di dati fanno piena prova dei fatti che attestano"*. A rafforzarne il valore probatorio, l'art. 179 CPC prevede che *"I registri pubblici e i documenti pubblici fanno piena prova dei fatti che attestano, finché non sia dimostrata l'inesattezza del loro contenuto"*. Infine e a ulteriore sostegno della valenza probatoria della copia scansionata, si può aggiungere come ai sensi del CPC *"Le copie in forma elettronica possono persino essere considerate documenti originali, segnatamente se la loro archiviazione è conforme alle norme previste dal diritto commerciale (vedi Ordinanza sui libri di commercio del 24 aprile 2002 [RS 221.431] e in particolare le disposizioni che prevedono l'applicazione di quei procedimenti tecnici [ad esempio, l'uso della firma digitale] che garantiscono l'integrità delle informazioni registrate). Se la parte interessata è in grado di dimostrare che tali norme sono state rispettate, la distinzione tra originale e copia diventa irrilevante."* La situazione ad oggi è tale che i documenti del personale vengono scansionati e in seguito distrutti, oltre che dall'amministrazione federale, anche da diversi Cantoni e città, segnatamente dai Cantoni Berna, Argovia, Grigioni e dalle città di Zurigo e Zugo. Riservate le condizioni dell'archiviazione poste dagli Archivi di Stato, gli altri documenti cartacei possono essere distrutti una volta avvenuta la loro digitalizzazione.

## **Art. 84b (nuovo)**

L'art. 84b prevede la trasmissione sistematica, vale a dire regolare e/o duratura, di dati riguardanti il personale pubblico, e in particolare la facoltà di far capo alla procedura di richiamo per specifiche unità amministrative (lett. c, d ed e), per i funzionari dirigenti e il personale a loro sottoposto ed espressamente designato. Ciò è indispensabile alla gestione dei dipendenti pubblici, con particolare riferimento ai doveri definiti all'art. 24 cpv. 1 e 2 LORD, secondo cui i funzionari dirigenti delle singole unità amministrative organizzano, dirigono, coordinano i loro dipendenti diretti e ne verificano la prestazione lavorativa. I funzionari dirigenti possono a loro volta designare persone di fiducia, quali i membri di organi scolastici oppure il proprio personale amministrativo (ad es., collaboratori/trici di direzione oppure segretari/e), e richiedere ai Servizi centrali che essi accedano ai dati tramite procedura di richiamo.

La necessità di dati personali e la rispettiva portata devono essere prima valutati dai Servizi centrali e dalla Sezione delle scuole comunali per ogni singolo utente che ne fa richiesta scritta e motivata, in funzione dei compiti legali adottati. L'articolo 84b riveste una notevole importanza soprattutto per quanto riguarda lo scambio di dati tra gli organi responsabili e le unità amministrative, poiché possono essere resi accessibili tramite procedura di richiamo, senza cioè che ogni richiesta debba essere valutata singolarmente e ogni trasmissione operata manualmente.

Oltre alle condizioni giuridiche, la procedura di richiamo è soggetta a precise condizioni tecniche, in particolare l'identificazione, l'autenticazione e le misure di sicurezza atte a evitare l'accesso di terzi non autorizzati.

Per quanto riguarda l'art. 84b lett. e), si precisa che con il termine di Centro dei sistemi informativi, sono intese anche le ditte esterne che agiscono su suo mandato.

### **Art. 84c (nuovo)**

Questa norma definisce le condizioni per la trasmissione di dati in singoli casi e riguardante un set definito di dati personali di una o più persone per uno scopo specifico e limitato nel tempo. La trasmissione in singoli casi presuppone l'adempimento di un motivo giustificativo, che può essere una base legale, ma anche la necessità per l'adempimento di un compito legale oppure il consenso scritto, libero e informato della persona interessata (art. 6 cpv. 2 LPDP). La trasmissione di dati è preceduta da una richiesta scritta e motivata, con indicazione del compito legale addotto e delle concrete necessità di dati. L'organo responsabile dei dati, appurata l'esistenza di un motivo giustificativo, procede successivamente con la valutazione della richiesta, in particolare per quanto attiene all'estensione dei dati richiesti, prima di procedere alla trasmissione. Esempi in tal senso sono la trasmissione di dati relativi al versamento degli oneri sociali (AVS e AI) ai servizi preposti della Confederazione, di dati sui casi d'infortunio alle assicurazioni incaricate della gestione ai sensi della LAINF<sup>8</sup>, oppure di dati inerenti alla previdenza professionale trasmessi all'Istituto collettore secondo la Legge sulla previdenza professionale (LPP<sup>9</sup>).

### **Art. 84d (nuovo)**

Con l'art. 84d si garantisce agli organi di cui all'art. 84 cpv. 1 la facoltà di elaborare dati personali dei dipendenti pubblici per l'esecuzione di puntuali compiti, mansioni o iniziative d'interesse legittimo per i dipendenti, l'Amministrazione pubblica o anche la cittadinanza. Tali elaborazioni devono avvenire nel rispetto dei principi generali del diritto, in particolare dei principi della proporzionalità e finalità. In assenza di questi motivi giustificativi, dovrà essere richiesto e ottenuto il consenso libero e informato dei dipendenti interessati, valido comunque solamente per elaborazioni puntuali e non sistematiche (vedi art. 6 LPDP).

Si possono citare, quali esempi, la pubblicazione sul sito internet dell'Amministrazione cantonale della lista dei nomi, cognomi, unità amministrative e numeri di telefono dei dipendenti, per garantire – nell'interesse pubblico – i servizi al cittadino. Possono altresì essere pubblicati regolarmente, all'interno dell'Amministrazione cantonale (intranet), la lista dei mutamenti dei dipendenti, per una tempestiva e regolare informazione all'interno dell'Amministrazione pubblica sui movimenti intervenuti nel personale, così come elaborare puntualmente i dati necessari all'esecuzione di misure d'interesse per i dipendenti o per l'Amministrazione pubblica.

Va segnalato in particolare che per quanto riguarda l'ulteriore esempio della pubblicazione dei piani settimanali di lavoro dei docenti – pacifica la sua legittimità di principio – essa può

---

<sup>8</sup> RS 832.20.

<sup>9</sup> RS 831.40.

avvenire unicamente previa adozione di adeguate misure di sicurezza dei dati (login con parola chiave e nome utente). Si rammenta che i piani in questione possono essere comprensivi dei luoghi e delle materie insegnate, nonché di eventuali ulteriori informazioni specifiche all'insegnamento.

#### **Art. 84e (nuovo)**

Il Servizio medico del personale dello Stato è organizzativamente attribuito alla Sezione delle risorse umane (SRU). Tuttavia, a garanzia del segreto medico, è operativamente autonomo e indipendente dalla SRU. L'iter di raccolta e ulteriore elaborazione dei dati medici è predisposto in modo tale che nessun dato medico di dettaglio è portato a conoscenza dei Servizi centrali del personale, i quali ricevono unicamente le informazioni generiche necessarie alla gestione amministrativa del rapporto d'impiego. Per quanto riguarda la procedura di assunzione, i Servizi centrali del personale si limitano a raccogliere e a girare immediatamente al Servizio medico il questionario sullo stato di salute per l'assunzione alle dipendenze dello Stato. Il questionario contiene esclusivamente l'indicazione generica della presenza o meno di un disturbo della salute, che sarà se necessario approfondito esclusivamente dal Servizio stesso, il quale fornirà successivamente ai Servizi centrali del personale indicazioni relative unicamente all'idoneità per la funzione da ricoprire, senza dettagli di tipo medico-clinico<sup>10</sup>.

La gestione dei dati sulla salute avviene sia in modo cartaceo (cartelle sanitarie contenenti essenzialmente i documenti medici provenienti dall'esterno del Servizio medico), sia in modo elettronico (rapporti e valutazioni dello stesso Servizio medico).

Secondo il cpv. 1, i dati medici dei dipendenti possono essere elaborati unicamente da persone soggette al segreto medico (medici e ausiliari).

Nell'ordinamento cantonale, la valutazione dello stato di salute è riservata in modo esplicito al medico del personale. Al cpv. 2 invece, è trattato lo scambio con lo Stato quale datore di lavoro e quindi le informazioni che le persone sottoposte al segreto medico di cui al cpv. 1 possono comunicargli. Il medico è autorizzato a comunicare ai Servizi centrali del personale unicamente le conclusioni relative alla capacità lavorativa in generale o per l'esercizio di una determinata funzione, al grado d'inabilità (espressa in percentuale), alla sua causa generica (malattia o infortunio) e alla durata presumibile dell'inabilità. Le risultanze concrete di ordine medico, e quindi eventuali problemi di salute, sono invece di esclusivo dominio del medico del personale e tutelate dal segreto medico. Tali principi si applicano per analogia al servizio corrispettivo dello IAS per la propria unità amministrativa.

#### **Art. 84f (nuovo)**

Al primo capoverso, la norma prevede la proibizione della sorveglianza intesa come misura di controllo nominativo, in tempo reale e prolungato della sfera privata o personale del dipendente pubblico. In altre parole, riguardo in particolare l'uso d'internet sul posto di lavoro, non è lecito mettere sotto sorveglianza nominativa e in tempo reale – vale a dire del presente e futuro - un dipendente a partire dalla constatazione di un abuso o dalla nascita di un rispettivo sospetto concreto. È invece lecito, per confermare un sospetto di abuso, controllare in modo nominativo e retrospettivo le giornalizzazioni (logfiles) delle attività passate in internet. È altresì lecito, secondo il cpv. 2, la sorveglianza non nominativa, vale a dire il controllo in tempo reale e prolungato in modo anonimo o pseudonimo (quest'ultimo, comunque, non a tempo indeterminato), del rispetto delle norme sul corretto uso delle risorse informatiche. La sorveglianza avviene in modo anonimo quando i dati ripresi nelle giornalizzazioni delle attività in internet o di posta

---

<sup>10</sup> Art. 7 del Regolamento dei dipendenti dello Stato del 2 giugno 2014; RL 2.5.4.1.1.

elettronica non sono a carattere personale e non permettono un'identificazione dell'utente (sorveglianza anonima). La sorveglianza avviene invece in modo pseudonimizzato quando i dati soggetti a controllo contengono informazioni (ad esempio, l'indirizzo IP dei computer) che possono essere ricondotte a specifiche persone con l'ausilio di una tabella di corrispondenza.

La sorveglianza in modo pseudonimo avviene come fase successiva alla sorveglianza anonima, allorché quest'ultima ha rivelato degli abusi e l'organo responsabile intende chiarire se essi sono ripartiti su tutta l'unità amministrativa oppure unicamente su singoli dipendenti. Nel primo caso, l'organo responsabile si limita di principio a segnalare la constatazione d'abusi e a richiamare i dipendenti al rispetto delle norme sul corretto uso delle risorse informatiche. Nel secondo caso, invece, l'organo responsabile, d'intesa con il Centro sistemi informativi e la Sezione delle risorse umane, può procedere all'identificazione del o dei responsabili e al rispettivo sanzionamento. L'identificazione avviene con l'ausilio di una tabella di corrispondenza, che deve essere conservata separatamente dalle giornalizzazioni. La tabella di corrispondenza contiene la lista degli indirizzi IP e dei relativi nominativi dei dipendenti. La comparazione delle giornalizzazioni con la lista delle corrispondenze, definibile anche come de-pseudonimizzazione o re-identificazione, può avvenire unicamente successivamente al rilevamento di un abuso delle risorse informatiche o alla nascita di un sospetto concreto di abuso durante la sorveglianza anonima o pseudonima. L'identificazione e la sanzione di un dipendente può avvenire anche successivamente alla constatazione di altri indizi quali il ritrovamento di stampati privati presso la stampante di servizio. In ogni caso, però, il datore di lavoro, e per esso i servizi informatici che garantiscono la disponibilità e il buon funzionamento delle risorse informatiche, devono prioritizzare la prevenzione degli abusi con adeguate misure di sicurezza (cpv. 4) tese, ad esempio, a bloccare l'accesso a determinati siti internet. La sorveglianza e l'eventuale, successiva identificazione di persone deve rimanere una misura del tutto secondaria (ultima ratio) rispetto alle misure di sicurezza. Infine, più in generale, il capoverso 5 riprende l'art. 26 cpv. 2 dell'Ordinanza 3 concernente la legge sul lavoro<sup>11</sup>, vertente a garantire la salute e la libertà di movimento dei dipendenti, e con ciò la loro personalità<sup>12</sup>, qualora sistemi di sorveglianza e di controllo sono implementati per altri fini (ad esempio, per il controllo della sicurezza tramite videosorveglianza).

### **Art. 84g (nuovo)**

Per i dossier di candidatura, riservato il diritto procedurale in caso di contenzioso, i documenti dei candidati non assunti e di proprietà del candidato sono eliminati trascorsi 3 mesi dal termine della procedura di assunzione (cpv. 1), ad eccezione dei dati anagrafici (nome, cognome, indirizzo e dati di contatto) e dello scritto contenuti nella lettera di motivazione e presentazione del candidato, che – quali parti integranti della corrispondenza indirizzata al datore di lavoro – sono conservati per 1 anno. I dati sono successivamente conservati in forma anonimizzata a scopo statistico.

I dati dei dipendenti sono conservati di principio per 10 anni dalla cessazione del rapporto d'impiego (cpv. 2). Tale periodo di conservazione – previsto anche presso altri Cantoni e la Confederazione – permette la ricostruzione del passato lavorativo in caso di necessità (ad esempio, nel contenzioso). Oltre il termine di 10 anni, i dati possono essere conservati unicamente con il consenso scritto, libero e informato del dipendente.

Al cpv. 3 sono definiti i dati la cui conservazione si protrae oltre i 10 anni di cui al cpv. 2. In caso di riassunzione tali dati permettono all'Amministrazione cantonale di adempiere, nell'interesse del dipendente, a compiti previsti dalle normative in vigore, quali ad esempio il computo degli anni di servizio per la gratifica d'anzianità.

---

<sup>11</sup> OLL 3; RS 822.113.

<sup>12</sup> DTF 130 II 425, consid. 3.3.

La conservazione di dati a scopi statistici e di ricerca è disciplinata dalla LPDP (art. 15), che è riservata all'art. 84h.

Raggiunto il termine di conservazione, i dossier personali – sia quelli in forma cartacea ancora a disposizione dei Servizi centrali sia quelli digitalizzati – dei dipendenti sono proposti all'Archivio di Stato, che ne valuta il valore archivistico conformemente alla Legge sull'archiviazione e sugli archivi pubblici del 15 marzo 2011<sup>13</sup>. Nel caso in cui i dossier non dovessero essere archiviati oppure lo dovessero essere solo in parte, i Servizi centrali provvedono alla loro distruzione. I dossier digitalizzati seguono le stesse regole dei dossier cartacei.

#### **Art. 84h (nuovo)**

Nella misura in cui la LORD non disciplina determinati aspetti della protezione dei dati nell'ambito del personale pubblico, si applica la LPDP.

#### **Art. 84i (nuovo)**

L'art. 84i delega al Consiglio di Stato il disciplinamento delle norme materiali d'esecuzione. Vanno previsti in particolare:

- per i sistemi d'informazione, i diritti di accesso tramite procedura di richiamo (segnatamente, le categorie di dati accessibili e l'utenza) con le rispettive giornalizzazioni;
- le modalità della candidatura elettronica e della digitalizzazione dei documenti cartacei e le misure di garanzia dell'autenticità del documento scansionato;
- le misure di sicurezza a garanzia della confidenzialità, dell'integrità e dell'autenticità dei dati e la loro conservazione;
- la procedura di analisi dei dati sull'utilizzo dell'infrastruttura elettronica secondo l'art. 84f e il servizio responsabile.

### **VIII. MODIFICHE DI ALTRE LEGGI**

Il Dipartimento dell'educazione, della cultura e dello sport, per il tramite delle competenti unità amministrative, gestisce tre differenti banche dati: quella dedicata alla gestione amministrativa dei docenti cantonali (GAS cantonale), quella dedicata alla gestione amministrativa dei docenti comunali (GAS comunale) e quella finalizzata alla gestione amministrativa e del curriculum formativo degli allievi e alla gestione amministrativa degli istituti scolastici e dei relativi Servizi centrali (GAGI). Attualmente queste banche dati trovano il loro fondamento giuridico nella Legge della scuola (art. da 91a a 91e).

Il Consiglio di Stato ha deciso di unificare nella LORD tutte le normative sull'elaborazione dei dati dei dipendenti soggetti alla legge, e quindi compresi i docenti cantonali, comunali e i direttori e vicedirettori delle scuole cantonali, al fine di garantire la parità di trattamento fra le diverse categorie di dipendenti. Con la presente revisione vengono pertanto scorporate dalla Legge della scuola le disposizioni inerenti le elaborazioni di dati concernenti i docenti. Le disposizioni della Legge della scuola che subiscono una modifica sono gli art. 91a-d, compreso il titolo IX, che è mutato in "Banca dati". Per il resto, le normative sulla gestione dei dati degli allievi (banca dati GAGI) non sono toccate dalla presente revisione.

---

<sup>13</sup> LArch; RL 1.6.2.1.

## **IX. RELAZIONE CON LE LINEE DIRETTIVE E IL PIANO FINANZIARIO**

La modifica legislativa non è contemplata dalle Linee direttive di legislatura, ma risulta necessaria in seguito alla terza revisione della LPDP (art. 6), entrata in vigore il 1° gennaio 2016.

Non sono previste conseguenze di natura finanziaria.

## **X. COMPATIBILITÀ CON LE ALTRE LEGGI CANTONALI E FEDERALI**

Le nuove norme ossequiano l'obbligo imposto dalla LPDP di una base legale nel diritto formale settoriale per le elaborazioni sistematiche di dati personali meritevoli di particolare protezione (art. 6 LPDP) e la loro accessibilità tramite procedura di richiamo (art. 14 cpv. 3 LPDP) e sono rispettose del diritto federale in materia di protezione dati.

Considerato quanto esposto, il Consiglio di Stato invita il Parlamento ad approvare i disegni di legge allegati al presente messaggio.

Vogliate gradire, signor Presidente, signore e signori deputati, l'espressione della nostra massima stima.

Per il Consiglio di Stato:

Il Presidente, Manuele Bertoli

Il Cancelliere, Arnoldo Coduri

Disegno di

## **LEGGE**

**sull'ordinamento degli impiegati dello Stato e dei docenti del 15 marzo 1995;  
modifica**

Il Gran Consiglio  
della Repubblica e Cantone Ticino

visto il messaggio 17 gennaio 2018 n. 7488 del Consiglio di Stato,

## **d e c r e t a :**

### **I.**

La legge sull'ordinamento degli impiegati dello Stato e dei docenti del 15 marzo 1995 è così modificata:

#### **Art. 13 cpv. 1 e 2**

<sup>1</sup>I candidati presentano la candidatura, se non specificato altrimenti, in forma elettronica completa dei documenti indicati nel bando di concorso.

<sup>2</sup>*Abrogato.*

#### **Art. 31a**

Il dipendente che, nell'esercizio delle sue funzioni, ha notizia di un reato di azione pubblica, è tenuto a farne immediato rapporto al Consiglio di Stato o al Ministero pubblico, trasmettendogli i verbali e gli atti relativi; qualora ne informi il Consiglio di Stato, quest'ultimo è tenuto a trasmettere immediatamente la segnalazione al Ministero pubblico.

## **TITOLO IV Protezione dei dati**

#### **Art. 84 (nuovo)**

#### **Sistemi d'informazione**

<sup>1</sup>I Servizi centrali del personale e l'unità amministrativa competente per la gestione amministrativa dei docenti comunali sono gli organi responsabili dell'elaborazione dei dati necessari alla gestione del personale e degli stipendi. Essi gestiscono sistemi d'informazione e di documentazione informatizzati per:

- a) la gestione delle candidature ai concorsi pubblici;
- b) la gestione e l'amministrazione del personale;
- c) l'allestimento di statistiche.

<sup>2</sup>Gli organi responsabili accedono ai dati elaborati nei sistemi d'informazione in funzione delle necessità per l'adempimento dei rispettivi compiti di gestione del personale.

<sup>3</sup>I sistemi d'informazione possono contenere in particolare dati relativi alla candidatura, alla carriera professionale, alle procedure amministrative, agli stipendi, alla gestione delle presenze e assenze, compresi dati personali meritevoli di particolare protezione, segnatamente relativi alla sfera familiare, allo stato di salute, alle valutazioni sulle prestazioni e sul comportamento professionali e alle procedure e sanzioni disciplinari e penali.

<sup>4</sup>Il Centro sistemi informativi e il Servizio informatica dell'Istituto delle assicurazioni sociali garantiscono la gestione e la sicurezza tecnica dei sistemi d'informazione.

#### **Art. 84a (nuovo)**

##### **Digitalizzazione dei documenti cartacei**

Gli organi responsabili possono digitalizzare e riprendere nei sistemi d'informazione i documenti cartacei. La copia digitale del documento, con le necessarie misure di sicurezza, è presunta equivalente all'originale cartaceo. In seguito, l'originale cartaceo può essere distrutto.

#### **Art. 84b (nuovo)**

##### **Trasmissione sistematica di dati**

<sup>1</sup>Gli organi responsabili possono trasmettere regolarmente, se del caso tramite procedura di richiamo, i dati personali necessari all'adempimento dei seguenti compiti legali:

- a) ai funzionari dirigenti e al personale espressamente designato, per la gestione delle unità amministrative e del personale attribuiti;
- b) ai funzionari dirigenti e al personale espressamente designato, per la gestione amministrativa dei docenti;
- c) all'Istituto di previdenza del Cantone Ticino, per la gestione della previdenza professionale degli assicurati;
- d) alle unità amministrative responsabili del recupero di sussidi e della contabilità analitica;
- e) al Centro sistemi informativi e al Servizio informatica dell'Istituto delle assicurazioni sociali, per lo sviluppo e il mantenimento di sistemi informativi contenenti dati dei dipendenti.

<sup>2</sup>È riservata la trasmissione sistematica di dati personali secondo altre leggi.

#### **Art. 84c (nuovo)**

##### **Trasmissione puntuale di dati**

Gli organi responsabili possono trasmettere, in singoli casi, dati personali ad organi pubblici o a privati se è previsto dalla legge, se sussiste una necessità per l'adempimento di compiti legali o se la persona interessata ha dato il suo consenso scritto, libero e informato.

#### **Art. 84d (nuovo)**

##### **Altre elaborazioni di dati**

Gli organi responsabili possono elaborare dati del personale per scopi che esulano da quelli previsti all'art. 84 cpv. 1, se ciò è necessario per l'adempimento di compiti legali o in garanzia d'interessi legittimi dei dipendenti o dell'Amministrazione pubblica.

#### **Art. 84e (nuovo)**

##### **Dati personali relativi alla salute**

<sup>1</sup>Il Servizio medico del personale dell'Amministrazione cantonale, come pure il servizio corrispettivo dello IAS per la propria unità amministrativa, sono gli organi responsabili dell'elaborazione dei dati personali sulla salute dei dipendenti, in particolare quelli relativi alla valutazione della loro idoneità lavorativa e al loro accompagnamento medico.

<sup>2</sup>Essi possono comunicare agli organi di cui all'art. 84 cpv. 1 unicamente le conclusioni attinenti all'idoneità rispettivamente inidoneità lavorativa della persona interessata, al grado, alla causa e alla durata presumibile dell'inabilità lavorativa e eventuali altre conclusioni necessarie all'assunzione e alla gestione del rapporto d'impiego.

#### **Art. 84f (nuovo)**

##### **Sorveglianza sul posto di lavoro**

<sup>1</sup>Non è ammesso l'impiego di sistemi di sorveglianza nominativa, durevole e in tempo reale della sfera privata o personale dei dipendenti sul posto di lavoro.

<sup>2</sup>La violazione di norme comportamentali sull'uso delle risorse informatiche, o il relativo sospetto, va constatato tramite una sorveglianza non nominativa dei dati raccolti, o grazie ad indizi fortuiti.

<sup>3</sup>È ammessa l'analisi nominativa puntuale dei dati personali raccolti tramite sistemi di sorveglianza, in caso di constatazione o di relativi sospetti concreti di violazione delle norme comportamentali secondo il cpv. 2.

<sup>4</sup>Il servizio responsabile della sicurezza adotta le misure tecniche e organizzative necessarie per prevenire gli abusi.

<sup>5</sup>I sistemi di sorveglianza o di controllo, se sono necessari per altre ragioni, devono essere concepiti e disposti in modo da non pregiudicare la salute e la libertà di movimento dei dipendenti.

#### **Art. 84g (nuovo)**

##### **Conservazione dei dati**

<sup>1</sup>I dati dei candidati non assunti sono eliminati dopo tre mesi dal termine della procedura di assunzione, ad eccezione della lettera di candidatura e dei dati anagrafici ivi contenuti che, in quanto corrispondenza indirizzata al datore di lavoro, sono conservati per un anno.

<sup>2</sup>I dati personali dei dipendenti possono essere conservati dieci anni dalla fine del rapporto d'impiego. Altri dati possono essere conservati oltre questo termine con il consenso scritto, libero e informato del dipendente.

<sup>3</sup>Sono conservati per una durata di trenta anni ai fini di un'eventuale riassunzione i dati anagrafici, l'allocazione organizzativa, la funzione ricoperta, l'entrata in servizio e le mutazioni nella carriera del dipendente.

<sup>4</sup>I dati del personale possono essere conservati in forma anonimizzata a scopo statistico.

#### **Art. 84h (nuovo)**

##### **Diritto suppletivo**

Rimangono riservate le disposizioni della legge sulla protezione dei dati personali del 9 marzo 1987.

#### **Art. 84i (nuovo)**

##### **Disposizioni esecutive**

Il Consiglio di Stato disciplina i particolari, segnatamente i diritti e le modalità di accesso ai sistemi d'informazione tramite procedura di richiamo, la digitalizzazione dei documenti cartacei, le modalità di conservazione, le misure di sicurezza dei dati e la procedura di analisi dei dati sull'utilizzo dell'infrastruttura elettronica secondo l'art. 84f.

## **II.**

<sup>1</sup>Trascorsi i termini per l'esercizio del diritto di referendum, la presente modifica di legge è pubblicata nel Bollettino ufficiale delle leggi.

<sup>2</sup>Il Consiglio di Stato ne fissa l'entrata in vigore.

Disegno di

## **LEGGE**

**della scuola del 1° febbraio 1990; modifica**

Il Gran Consiglio  
della Repubblica e Cantone Ticino

visto il messaggio 17 gennaio 2018 n. 7488 del Consiglio di Stato,

## **d e c r e t a :**

### **I.**

La legge della scuola del 1° febbraio 1990 è così modificata:

#### **Titolo X Banca dati**

##### **Art. 91a**

**Sistema  
d'informazione  
per la gestione  
degli allievi e  
degli istituti**

<sup>1</sup>Il Dipartimento competente, tramite le unità amministrative definite dal regolamento, gestisce la banca dati «Gestione allievi gestione istituti» (GAGI), per la gestione amministrativa e del curriculum formativo degli allievi, nonché per la gestione amministrativa degli istituti scolastici e dei relativi servizi centrali.

<sup>2</sup>La banca dati GAGI contiene i dati personali necessari all'adempimento dei compiti legali degli organi interessati, inclusi dati meritevoli di particolare protezione, segnatamente relativi allo stato di salute, alle sanzioni penali limitatamente all'iscrizione a casellario giudiziale e amministrative, ai provvedimenti disciplinari, nonché alla sfera familiare se strettamente necessari per la gestione ordinaria della scuola.

<sup>3</sup>La banca dati GAGI può servire all'allestimento di statistiche.

##### **Art. 91b lett. a) e c)**

- a) quelli necessari all'adempimento dei compiti di gestione degli allievi ai membri di organi scolastici e di conduzione degli istituti nonché al loro personale amministrativo;
- c) quelli necessari all'adempimento dei compiti di gestione degli allievi ai singoli servizi dipartimentali;

##### **Art. 91c cpv. 1 e 2**

<sup>1</sup>I dati personali inerenti ad allievi possono essere trasmessi a organi pubblici solo se l'autorità competente è autorizzata dalla legge e se i dati nel caso specifico sono indispensabili all'organo richiedente per l'adempimento dei suoi compiti legali oppure se la persona interessata o il suo rappresentante legale, nel singolo caso, hanno dato il loro consenso libero e informato.

<sup>2</sup>La trasmissione a privati di dati personali di allievi, liste di classe comprese, è possibile solo se l'autorità competente è autorizzata dalla legge, oppure se la persona interessata o il suo rappresentante legale hanno dato il loro consenso libero e informato.

**Art. 91d cpv. 2**

<sup>2</sup>*Abrogato.*

**II.**

<sup>1</sup>Trascorsi i termini per l'esercizio del diritto di referendum, la presente modifica di legge è pubblicata nel Bollettino ufficiale delle leggi.

<sup>2</sup>Il Consiglio di Stato ne fissa l'entrata in vigore.