

**LE FONTI DEL DIRITTO ITALIANO**

I testi fondamentali commentati con la dottrina  
e annotati con la giurisprudenza

# **CODICE DELLA PRIVACY E DATA PROTECTION**

a cura di

**R. D'Orazio – G. Finocchiaro  
O. Pollicino – G. Resta**

con la collaborazione di  
G. De Gregorio

 **GIUFFRÈ**  
GIUFFRÈ FRANCIS LEFEBVRE

ISBN 9788828822561

© Copyright Giuffrè Francis Lefebvre S.p.A. Milano - 2021  
Via Busto Arsizio, 40 - 20151 MILANO - [www.giuffrefrancislefebvre.it](http://www.giuffrefrancislefebvre.it)  
Chiuso in redazione il 4 giugno 2021

La traduzione, l'adattamento totale o parziale, la riproduzione con qualsiasi mezzo (compresi i microfilm, i film, le fotocopie), nonché la memorizzazione elettronica, sono riservati per tutti i Paesi.

L'Editore declina ogni responsabilità per eventuali refusi o inesattezze presenti nel volume pur curato con la massima diligenza e attenzione.

---

Stampato da Galli Edizioni S.r.l. - Varese

## PREFAZIONE

1. Il diritto alla privacy e alla tutela dei dati personali sollecita ormai sempre maggiore attenzione da parte del giurista in considerazione dei recenti sviluppi tecnologici, economici e sociali. L'utilizzo dei dati nella società dell'informazione ha condotto a un miglioramento della prestazione dei servizi pubblici e supportato l'emersione di nuovi modelli di business, favorendo innovazione e crescita economica. Tuttavia, allo stesso tempo, tali opportunità hanno costituito anche un rischio per il costituzionalismo democratico che, come mostrato dal caso *Cambridge Analytica*, è sempre più insidiato dalla sproporzione nella distribuzione del potere sociale, spesso derivante dal controllo esclusivo su masse enormi di dati. In una società dove le tecnologie digitali rivestono sempre più un ruolo centrale, è inevitabile indagare se il paradigma europeo di tutela della privacy e dei dati personali, che tende a impostarsi come standard regolatorio globale secondo il paradigma del Brussels effect, sia al passo rispetto alle nuove tendenze dell'economia digitale o, più in particolare, del capitalismo digitale.

Tuttavia, il percorso che ha portato all'emersione e al consolidamento del diritto alla privacy e alla tutela dei dati personali come valori fondamentali dell'Unione nella società digitale non inizia nel vecchio continente ma trova la sua origine oltre oceano. Quel *right to be let alone* teorizzato da Warren and Brandeis alla fine del XIX secolo nel contesto statunitense ha subito un processo di migrazione ed evoluzione nel contesto europeo. Dapprima, il diritto alla privacy ha trovato fondamento nell'art. 7 della Convenzione europea dei diritti dell'uomo nella sua connotazione di rispetto della vita privata e familiare. Da qui, complice l'ampiamiento delle burocrazie dello stato sociale nonché dello sviluppo delle tecnologie di trattamento delle informazioni, tra cui Internet, il diritto alla privacy ha subito un processo di evoluzione che ha portato all'emersione di una dimensione positiva o, dinamica consistente nella tutela dei dati personali.

Anche spinta dall'adozione in sede nazionale di normative a tutela dei dati personali e, dalla giurisprudenza della Corte di Strasburgo, nel 1995, l'Unione adottava la Direttiva 95/46/CE ossia il primo strumento sovranazionale in materia di *data protection*. Soltanto qualche anno dopo, il diritto alla privacy e alla tutela dei dati personali veniva recepito negli artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione adottata nel 2000. Il riconoscimento formale della sua forza giuridica obbligatoria allo stesso livello dei Trattati, conseguente all'entrata in vigore del Trattato di Lisbona nel 2009, ha costituito un momento fondamentale per il consolidamento del diritto alla privacy e alla tutela dei dati personali nella dimensione costituzionale europea.

Soprattutto a seguito di questo decisivo passaggio formale, non è mancato l'intervento della Corte di giustizia a consolidare la tutela costituzionale di tali diritti in almeno tre decisioni chiave, in particolare *Digital Rights Ireland*, *Google Spain* and *Schrems*. Tali decisioni testimoniano una forma di *judicial activism*, che ha cercato di colmare le lacune di un quadro legislativo ormai non al passo con le sfide della società digitale. Questa fase ha inoltre costituito un ponte verso l'adozione di un nuovo sistema di tutela dei dati personali in

Europa con l'adozione del Regolamento UE 679/2016 che sempre di più costituisce un modello su scala globale.

Il GDPR ha segnato un momento di distacco dell'approccio europeo dalla mera dimensione economico-funzionale del diritto alla tutela dei dati personali come mezzo per favorire la crescita del mercato interno attraverso la circolazione dei dati. Il GDPR ha segnato una svolta verso una strategia che mira non solo ai fini del mercato ma anche, e soprattutto, alla tutela dei diritti fondamentali che costituiscono un punto di riferimento per l'intero nuovo sistema normativo. Il GDPR, attraverso i principi generali, i nuovi obblighi posti in capo ai titolari del trattamento e i diritti stabiliti a protezione degli interessati, definisce un quadro di tutela dei dati personali interamente rinnovato e basato su un *risk-based approach*, che pone al centro la responsabilizzazione del titolare del trattamento.

2. Un tale percorso ha attirato l'attenzione al tema della privacy e alla tutela dei dati personali, come dimostrato anche dal numero di volumi e ricerche in materia, nonché dei vari commentari dedicati al GDPR e alla normativa collegata. Tra questi meritano di essere specificamente menzionati KUNER, BYGRAVE, DOCKSEY (eds.), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford, 2020; FEILER, FORGÓ, WEIGL (eds.), *The EU General Data Protection Regulation (GDPR): A Commentary*, Globe Law and Business, 2018; PAAL-PAULY, *Datenschutz-Grundverordnung*, München, 2017. Anche a livello nazionale l'attenzione è stata posta ampiamente sul GDPR, come esemplificato da CUFFARO, D'ORAZIO, RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, 2019; PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al regolamento UE n. 2016/679 (GDPR) e al novellato D.lgs. n. 196/2003 (Codice privacy)*, Milano 2019; RICCIO, SCORZA, BELISARIO (a cura di), *GDPR e Normativa Privacy Commentario*, Milano, 2018; FINOCCHIARO (diretto da), *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna 2017; PELINO, BISTOLFI, BOLOGNINI (a cura di), *Il regolamento privacy europeo. Commentario alla nuova disciplina europea sulla protezione dei dati, in vigore da maggio 2016*, Milano 2016. Il presente commentario mira ad arricchire questo percorso di ricerca fornendo una prospettiva sistematica del diritto alla tutela della privacy e dei dati personali nel contesto sovranazionale e nazionale europeo. Tra i tratti distintivi dell'opera, occorre menzionare che l'analisi non si limita al GDPR, ma offre un quadro analitico di tutta la normativa nazionale in materia, e in primo luogo del d.lgs. n. 196/2003 (Codice in materia di protezione dei dati personali) e del d.lgs. n. 101/2018. Inoltre, essa non si sofferma solo sul cambiamento del paradigma di tutela introdotto dal GDPR ma esamina anche l'evoluzione e l'applicazione della disciplina sin dalla sua adozione, con particolare attenzione ai casi giurisprudenziali, ai provvedimenti delle autorità competenti e ai riferimenti dottrinali. Infine, l'attenzione particolare in apertura alla tutela dei diritti fondamentali nel sistema della Convenzione europea e della Carta di Nizza costituisce una prospettiva unica per lo studio di un sistema tipicamente multilivello e che non può essere letto soltanto dal punto delle regole del GDPR o da una prospettiva nazionale.

Tale cornice costituzionale fornisce quindi all'opera quell'orientamento che permette di esaminare la disciplina attraverso un angolo prospettico che guida l'interpretazione dei commenti contenuti nell'opera. Più in particolare, la prima parte del commentario fornisce il quadro internazionale analizzando la tutela della privacy e dei dati personali nel contesto della Convenzione europea dei diritti fondamentali e della Carta di Nizza. Una volta esaminata la portata di tali diritti fondamentali in Europa, l'analisi si focalizza sul GDPR, fornendo quindi un commento analitico degli articoli che ne compongono la sua struttura. I commenti della normativa internazionale e sovranazionale sono inoltre accompagnati dall'analisi dettagliata della disciplina nazionale che, all'indomani dell'adozione del GDPR,

PREFAZIONE

---

5. I Curatori desiderano ringraziare particolarmente il dott. Giovanni De Gregorio per la preziosa collaborazione e il supporto, nonché la casa editrice Giuffrè Francis Lefebvre per la flessibilità e la capacità di adattamento mostrate nel complesso contesto pandemico.

Milano, Bologna, Roma

ROBERTO D'ORAZIO, GIUSELLA FINOCCHIARO, ORESTE POLLICINO, GIORGIO RESTA

Dando applicazione all'art. 8 l. n. 300/1970, la Suprema Corte ha poi escluso la legittimità della **clausola del bando di concorso** per l'assunzione di nuovo personale da parte di un ente pubblico economico, che limiti la partecipazione al concorso ai figli di dipendenti e di ex dipendenti, subordinando l'assunzione dei candidati, ove vincitori, alla preventiva cessazione del rapporto di lavoro dei congiunti (CC 9 marzo 2012 n. 3831).

### Capo III

#### CONTROLLO A DISTANZA, LAVORO AGILE E TELELAVORO <sup>(1)</sup>

<sup>(1)</sup> Rubrica sostituita dall'art. 9, comma 1, lett. e), d.lgs. 10 agosto 2018, n. 101

#### 114 **Garanzie in materia di controllo a distanza** <sup>(1)</sup>. — 1. *Resta fermo quanto disposto dall'articolo 4 della legge 20 maggio 1970, n. 300.*

<sup>(1)</sup> Rubrica sostituita dall'art. 9, comma 1, lett. g), d.lgs. 10 agosto 2018, n. 101.

#### 115 **Telelavoro, lavoro agile e lavoro domestico** <sup>(1)</sup>. — 1. *Nell'ambito del rapporto di lavoro domestico del telelavoro e del lavoro agile il datore di lavoro è tenuto a garantire al lavoratore il rispetto della sua personalità e della sua libertà morale* <sup>(2)</sup>. 2. *Il lavoratore domestico è tenuto a mantenere la necessaria riservatezza per tutto quanto si riferisce alla vita familiare.*

<sup>(1)</sup> Rubrica sostituita dall'art. 9, comma 1, lett. h), d.lgs. 10 agosto 2018, n. 101.

<sup>(2)</sup> Comma modificato dall'art. 9, comma 1, lett. h), d.lgs. 10 agosto 2018, n. 101.

Commento di **ARTURO MARESCA**

#### BIBLIOGRAFIA

ALVINO, *I nuovi limiti al controllo a distanza dell'attività dei lavoratori nell'intersezione tra le regole dello Statuto dei lavoratori e quelle del Codice della privacy*, *Labour&Law Issues*, 2016, vol. 2, I, 9; BALLETTI, *I poteri del datore di lavoro tra legge e contratto*, *DML*, 2018, 63; BARBIERI, *L'utilizzabilità delle informazioni raccolte: il Grande Fratello può attendere (forse)*, in TULLINI (a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore*, Torino, 2017, 183; BELLAVISTA, *Il nuovo art. 4 dello statuto dei lavoratori*, in ZILIO GRANDI-BIASI (a cura di), *Commentario breve alla riforma "Jobs Act"*, Padova, 2016, 717; CALIFANO, *Tecnologie di controllo del lavoro: limiti, procedure, garanzie*, in TULLINI (a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore*, Torino, 2017, 165; CARINCI M.T., *Il controllo a distanza sull'adempimento della prestazione di lavoro*, in TULLINI (a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore*, Torino, 2017, 50; COLAPIETRO, *Tutela della dignità e riservatezza del lavoratore nell'uso delle tecnologie digitali per finalità di lavoro*, *GDLRI*, 2017, 439; DEL PUNTA, *La nuova disciplina dei controlli a distanza sul lavoro (art. 23, d.lg. n. 151/2015)*, *RIDL*, 2016, I, 77; GAETA, *Telelavoro*, *EGT*, Diritto on-line, 2015; GRAGNOLI, *Gli strumenti di controllo e i mezzi di produzione*, *Variazioni sul tema di diritto del lavoro*, 2016, 651; INGRAO, *Il controllo a distanza sui lavoratori e la nuova disciplina privacy: una lettura integrata*, Bari, 2018; LAMBERTUCCI, *Potere di*

controllo del datore di lavoro e tutela della riservatezza del lavoratore: i controlli "a distanza" tra attualità della disciplina statutaria, promozione della contrattazione di prossimità e legge delega del 2014 (c.d. Jobs Act), C.S.D.L.E. It., n. 155/2015; MAIO, *La nuova disciplina dei controlli a distanza sull'attività dei lavoratori e la modernità post panottica*, ADL, 2015, 1186; MAINARDI, *Il potere disciplinare e di controllo sulla prestazione del lavoratore agile*, in FIORILLO-PERULLI (a cura di), *Il Jobs act del lavoro autonomo e del lavoro agile*, Torino, 2018, 213; MARAZZA, *Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore)*, C.S.D.L.E. It., n. 300/2016; MARESCA, *Controlli tecnologici e tutele del lavoratore nel nuovo art. 4 dello Statuto dei lavoratori*, RIDL, 2016, I, 513; NUZZO, *La protezione del lavoratore dai controlli impersonali*, Napoli, 2018; PINTO, *I controlli "difensivi" del datore di lavoro sulle attività informatiche e telematiche del lavoratore*, in TULLINI (a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore*, Torino, 2017, 139; PINTO, *La flessibilità funzionale e i poteri del datore di lavoro. Prime considerazioni sui decreti attuativi del cd. Jobs Act e sul lavoro agile*, RGL, 2016, I, 345; PROLA, *Trattamento dei dati personali, rapporto di lavoro e l'impatto della nuova disciplina dei controlli a distanza*, RIDL, 2016, I, 547; SALIMBENI, *La riforma dell'art. 4 dello Statuto dei lavoratori: l'ambigua risolutezza del legislatore*, RIDL, 2015, I, 589; SANTORO PASSARELLI, *Lavoro eterorganizzato, coordinato, agile e il telelavoro: un puzzle non facile da comporre in un'impresa in via di trasformazione*, C.S.D.L.E. It., n. 327/2017; TEBANO, *La nuova disciplina dei controlli a distanza: quali ricadute sui controlli conoscitivi?*, RIDL, 2016, I, 356; TIRABOSCHI, *Il lavoro agile tra legge e contrattazione collettiva: la tortuosa via italiana verso la modernizzazione del diritto del lavoro*, C.S.D.L.E. It., n. 335/2017; TROJSI, *Controllo a distanza (su impianti e strumenti di lavoro) e protezione dei dati del lavoratore*, Variazioni sul tema di diritto del lavoro, 2016, 4, 684; TULLINI, *La digitalizzazione del lavoro, la produzione intelligente e il controllo tecnologico nell'impresa*, in TULLINI (a cura di), *Web e lavoro. Profili evolutivi e di tutela*, Torino, 2017, 6; ZOLI, *Il controllo a distanza dell'attività dei lavoratori e la nuova struttura dell'art. 4, legge n. 300/1970*, Variazioni sul tema di diritto del lavoro, 2016, 635.

REFERIMENTI NORMATIVI: Artt. 3, 4, 8, l. n. 300/1970; artt. 18 ss. l. n. 81/2017; l. n. 877/1973.

### SOMMARIO

1. Il nuovo art. 4 l. n. 300/1970 alla luce del Regolamento UE 679/2016 e del d.lgs. n. 101/2018. — 2. La distinzione dei tre momenti della raccolta/acquisizione, della conservazione e dell'utilizzazione dei dati raccolti tramite strumenti di controllo a distanza. — 3. La (ri)definizione e sistematizzazione dei c.d. controlli difensivi. — 4. Condizioni di legittimità dei controlli a distanza: l'accordo sindacale e l'autorizzazione amministrativa. — 5. Le esenzioni riservate agli strumenti utilizzati per rendere la prestazione lavorativa e per la registrazione degli accessi e delle presenze. — 6. Controlli legittimi e utilizzabilità dei dati acquisiti per la gestione del rapporto di lavoro. — 7. L'informazione trasparente al lavoratore come condizione per l'utilizzabilità dei dati raccolti dal datore di lavoro. — 8. Tutela della riservatezza del lavoratore e del datore di lavoro nel telelavoro, nel lavoro agile e nel lavoro domestico.

**1. Il nuovo art. 4 l. n. 300/1970 alla luce del Regolamento UE 679/2016 e del d.lgs. n. 101/2018.** La disposizione in commento, il cui testo non è stato modificato dal d.lgs. n. 101/2018 che ne ha mutato solo la rubrica, fa salvo l'art. 4 l. n. 300/1970, il quale è destinato a definire i limiti entro i quali il datore di lavoro può impiegare in azienda strumenti in grado di controllare a distanza l'attività lavorativa dei propri dipendenti.

Se il testo della disposizione in commento non è stato modificato in sede di adeguamento della disciplina nazionale a quella europea, l'art. 4 richiamato ha invece subito un importantissimo aggiornamento nel 2015 (ad opera dell'art. 23 d.lgs. n. 151/2015 e dell'art. 5, comma 2, d.lgs. n. 185/2016), tramite il quale, tra le altre modifiche, è stato inserito all'interno del suo ultimo comma un espresso

rimando al Codice della privacy, laddove è prescritto che: “*le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d’uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal d.lgs. 196/2003*”.

Ne deriva un singolare “circolo normativo” in virtù del quale la disciplina di settore in materia di tutela della riservatezza rimette alla disciplina speciale lavoristica la regolamentazione del trattamento dei dati personali del lavoratore che sia realizzato in conseguenza dell’impiego di uno strumento idoneo a realizzare un controllo a distanza dell’attività lavorativa. Regolamentazione che, però, come prescrive la norma lavoristica, non è totalmente autonoma, essendo destinata ad integrarsi e coordinarsi con quella in materia di privacy, chiamando così l’interprete ad un’operazione ermeneutica non semplice.

In questa sede appare dunque utile svolgere un sintetico esame dei contenuti della disposizione dello Statuto dei lavoratori per approfondire in che modo la stessa sia destinata ad interagire con le regole del Codice della privacy.

Procedendo con ordine, va subito rilevato che le ragioni della recente modifica dell’art. 4, l. n. 300/1970 sono state tradizionalmente individuate nella obsolescenza della disciplina statutaria causata dalle nuove tecnologie (ALVINO, 2016, 4; TULLINI, 2017, 6) e forse, ancor più, dall’imponente evoluzione della normativa generale in materia di tutela della riservatezza (in particolare, il Codice e la sua implementazione da parte del Garante).

Volgendo lo sguardo al nuovo testo dell’art. 4 se ne può percepire, in grandi linee, l’evoluzione isolando almeno tre profili che evidenziano i tratti di continuità e discontinuità rispetto alla norma statutaria, quanto ad interessi tutelati e tecniche di regolamentazione.

Il primo concerne l’approccio al tema dei controlli a distanza tecnologici che conferma la volontà del legislatore di assoggettare questi controlli a limiti specifici finalizzati a tutelare la **riservatezza del dipendente**, escludendo la liberalizzazione di tali controlli.

Il secondo riguarda, nel segno della discontinuità, forme e strumenti di realizzazione della tutela del lavoratore che si caratterizzano per il **declino dell’accordo sindacale come condizione generale e sufficiente di legittimità dei controlli a distanza**. Infatti, il bene della riservatezza del lavoratore viene garantito dal legislatore in forme più coerenti alla dimensione individuale e personale di tale diritto, con attenzione per le modalità e la misura del controllo da correlare alle funzioni che esso legittimamente può assolvere. Ciò in perfetta coerenza con l’impostazione data alla regolazione del trattamento dal Regolamento UE 2016/679.

Il terzo profilo — che si pone in linea di sviluppo con quanto appena accennato — riguarda il raccordo, già più sopra anticipato, tra i controlli a distanza e l’utilizzabilità “*delle informazioni raccolte [...] a tutti i fini connessi al rapporto di lavoro*” (art. 4, comma 3). Un raccordo che chiarisce l’interazione funzionale dei poteri (in particolare, quelli di controllo e disciplinare) del datore di lavoro: da una parte il legittimo accertamento dell’infrazione e, dall’altra, la possibilità di sanzionarla. Affianco a tali profili, va considerato che, pur in mancanza di una disposizione analoga a quella che si leggeva nel testo originario del comma 1 dell’art. 4, il nuovo



testo continua a vietare al datore di lavoro di avvalersi di strumenti tecnologici per controllare a distanza la prestazione del dipendente, in quanto tali controlli sono ammessi "esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale" e, per converso, vietati in ogni altro e diverso caso (in tal senso CP 6 dicembre 2016 n. 51897, FI, 2017, 2, II, 89).

**2. La distinzione dei tre momenti della raccolta/acquisizione, della conservazione e dell'utilizzazione dei dati raccolti tramite strumenti di controllo a distanza.** Le considerazioni appena svolte consentono di mettere a fuoco alcune questioni che, specialmente nella fase applicativa della norma, hanno creato e potrebbero ancora creare incertezze e confusioni. Questioni di rilevante importanza per definire con chiarezza l'ambito della regolazione riservato alla disciplina in materia di privacy (Regolamento e Codice) rispetto a quello sul quale è destinato ad operare l'art. 4, l. n. 300/1970.

In questa logica, la prima questione, solo apparentemente banale, riguarda la **distinzione tra esercizio del controllo a distanza ed utilizzo dei dati derivanti da tale controllo**. Infatti, accade spesso che questi due aspetti vengano sovrapposti e percepiti come se fossero riconducibili ad un unico atto catalogabile come esercizio del potere di controllo. Ciò accade perché molto spesso l'avvenuto controllo, cioè l'acquisizione del dato, si manifesta in modo visibile soltanto quando si procede alla sua utilizzazione nei confronti del singolo lavoratore.

Per chiarire il punto occorre fare riferimento (almeno) a tre fasi cronologicamente e funzionalmente distinte: la prima riguarda l'**acquisizione** dei dati relativi all'attività lavorativa, come conseguenza automatica della tecnologia utilizzata dal dipendente per svolgere l'attività lavorativa; la seconda concerne la conservazione dei dati, cioè la loro **memorizzazione**; la terza — che è meramente eventuale — attiene all'**utilizzo** dei dati per la gestione del rapporto di lavoro. La sequenza delle tre fasi connota e caratterizza la tipologia dei controlli tecnologici prevista dall'art. 4; controlli che, appunto, vengono definiti « a distanza » per segnare lo spazio di luogo o di tempo che intercorre tra il momento o il luogo in cui il dato inerente all'attività lavorativa viene a formarsi, quello della raccolta/acquisizione, quello della conservazione e, infine, quello dell'utilizzazione.

I limiti posti dal nuovo art. 4 scandiscono bene (e, comunque, più nitidamente di quanto avveniva nella formulazione antecedente alle modifiche del 2015) le tutele del lavoratore con riferimento alle varie fasi, tenendo conto che il controllo a distanza si configura esaustivamente nel momento in cui il dato viene acquisito (e memorizzato), anche prescindendo dalla sua utilizzazione che è solo eventuale.

Si potrebbe ulteriormente precisare che, all'interno dell'art. 4, l'acquisizione del dato relativo all'attività lavorativa integra l'esercizio del potere di controllo secondo quanto stabilito dai commi 1 e 2; mentre il comma 3 detta le regole per l'utilizzazione del dato "a tutti i fini connessi al rapporto di lavoro" e ciò attiene non già al potere di controllo, bensì a quelli di gestione del rapporto di lavoro, in particolare (ma non solo) al potere disciplinare. Una distinzione che, peraltro, si riflette anche sul regime sanzionatorio previsto dall'art. 171 del Codice, che attribuisce rilievo penale alla violazione del solo comma 1 dell'art. 4 e non dei commi 2 e 3.

Alla stregua delle considerazioni accennate non appare quindi possibile sostenere, ad esempio, che i limiti al potere di controllo posti dall'art. 4 troverebbero applicazione e si attiverrebbero non già nel momento in cui lo « strumento » acquisisce il dato attinente all'attività lavorativa, ma soltanto quando tale dato, seppure già residente nella memoria di un server aziendale, viene esaminato per valutarne la rilevanza ai fini disciplinari, cioè nel caso della sua utilizzazione. La conseguenza di una simile impostazione sarebbe infatti paradossale: l'accordo sindacale o l'autorizzazione amministrativa dovrebbero essere richiesti soltanto se il datore di lavoro fosse interessato ad utilizzare il dato, mentre è proprio l'acquisizione di esso che pone il tema della tutela della riservatezza a presidio della quale opera l'art. 4. D'altronde una simile interpretazione si rivelerebbe incompatibile anche con quanto prescritto dal GDPR ed in particolare con il principio di minimizzazione dei dati che impone che i dati siano acquisiti, a prescindere dalla loro successiva catalogazione, solo in quanto necessari alla realizzazione delle finalità legittime che hanno giustificato il trattamento.

**3. La (ri)definizione e sistematizzazione dei c.d. controlli difensivi.** Prima di passare ad esaminare nel dettaglio i contenuti della nuova formulazione dell'art. 4 e a considerare il rapporto che intercorre tra le regole poste da tale disposizione e quelle dettate dal Codice e dal Regolamento, è opportuno affrontare immediatamente la questione riguardante la posizione che deve essere attribuita ai c.d. « controlli difensivi » rispetto al nuovo art. 4. È, infatti, necessario chiedersi se l'espressa inclusione della tutela del patrimonio aziendale, tra le esigenze che consentono l'installazione di strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori (ad opera dell'art. 23 d.lgs. n. 151/2015), abbia prodotto il definitivo assorbimento dei controlli difensivi nell'area di applicazione della disposizione statutaria, cosicché ora la realizzazione di tali controlli possa avvenire solo nel rispetto delle condizioni previste dal comma 1 (in tal senso: ALVINO, 2016, 9; BALLETTI, 2018, 63; LAMBERTUCCI, 2015, 9; NUZZO, 2018, 51 ss.). Ovvero, viceversa, se anche sotto il vigore della nuova formulazione, possa riconoscersi ai controlli difensivi uno statuto regolativo autonomo (cfr. in tal senso: MARAZZA, 2016, 18; MAIO, 2015, 1186; MARESCA, 2016, 513; PROIA, 2016, 547). Per fornire una risposta a tale quesito si può inizialmente osservare che i c.d. controlli difensivi sono stati utilizzati dalla giurisprudenza per sostenere l'inapplicabilità dell'art. 4 (vecchio testo) e, quindi, la legittimità del controllo anche in assenza del preventivo accordo sindacale, atteso che oggetto del controllo sarebbe stata non già l'attività lavorativa, bensì l'**illecito commesso in occasione della prestazione resa dal dipendente** al datore di lavoro.

Questa tesi — mutuata da quella che ammette, ex art. 3 l. n. 300/1970, i controlli occulti tramite agenzie investigative finalizzati ad accertare condotte penalmente rilevanti dei dipendenti durante il servizio (cfr., tra le più recenti: CC 22 maggio 2017, n. 12810, FI; CC 4 dicembre 2014, n. 25674, FI, 2015, I, 1671; CC 4 marzo 2014, n. 4984, NGL, 2014, 486; Nella giurisprudenza di merito v., da ultimo, T Padova, ord. 4 ottobre 2019) — sembra difficilmente armonizzabile con la rego-

lamentazione dei controlli tecnologici contenuta nell'art. 4, proprio per le modalità di funzionamento di tali controlli.

Infatti, mentre l'incarico affidato ad un'agenzia investigativa può essere circoscritto alle sole indagini necessarie ad accertare la condotta illecita del singolo dipendente ed essere considerato legittimo proprio perché così delimitato, viceversa il controllo tecnologico derivante, ad esempio, dall'utilizzo di un sistema informatico registra l'insieme di tutti i dati relativi all'attività lavorativa svolta indistintamente dalla generalità dei dipendenti senza alcuna selettività, né soggettiva né oggettiva.

In questo caso, quindi, non si può configurare un controllo difensivo, proprio perché il controllo non è focalizzato sull'attività illecita, ma indistintamente sulla prestazione lavorativa nel suo complesso resa da tutto il personale dipendente.

E non appare neppure possibile che tale qualificazione avvenga, per così dire a posteriori, cioè quando dall'analisi dei dati acquisiti riferita alla generalità dei lavoratori si riscontra una condotta illecita di un singolo dipendente.

Infatti, in questo caso il controllo a distanza è avvenuto quando sono stati acquisiti e memorizzati i dati relativi all'ordinaria attività lavorativa svolta dal personale dipendente ed a tale controllo trova sicura applicazione l'art. 4 la cui violazione rende illegittimo il controllo effettuato; senza alcuna possibilità che l'accertamento di comportamenti illeciti del dipendente in base ai dati complessivi già raccolti possa legittimare, con effetto retroattivo, il controllo ormai consumato.

Si può allora affermare, riprendendo le tre fasi più sopra evidenziate a cui fa riferimento la regolazione dettata dall'art. 4, che l'accertamento dell'illecito del lavoratore avviene nella fase di utilizzo dei dati a fini disciplinari, da distinguere da quella del controllo a distanza che si è consumata precedentemente con l'acquisizione dei dati.

Ciò non esclude, in assoluto, la possibilità di attivare un controllo realmente difensivo attraverso strumenti tecnologici al di fuori dell'ambito di applicabilità dell'art. 4, ma ciò può avvenire quando il sistema informatico (o una sua funzione) viene tarato in modo tale da accertare soltanto condotte illecite del dipendente e non già l'attività lavorativa nel suo complesso: ad esempio un software mirato a verificare l'autore di reati informatici.

Le considerazioni appena svolte consentono di ribadire che anche il nuovo art. 4 non si applica ai controlli difensivi — nel senso dei controlli aventi ad oggetto condotte illecite — che, conseguentemente, potranno essere attivati anche senza accordo sindacale o autorizzazione amministrativa.

Seguendo questa che sembra l'impostazione preferibile del problema, si può aggiungere che la previsione (art. 4, comma 1) dei controlli sul patrimonio aziendale dovrebbe consentire di ricondurre i controlli difensivi nel loro originario e corretto alveo.

Ciò potrebbe avvenire distinguendo tra: a) controlli a difesa del patrimonio aziendale costituito dai beni materiali ed immateriali di cui l'imprenditore ha la proprietà o il godimento e che riguardano la generalità dei dipendenti (o parte di essi) nello svolgimento della loro normale attività lavorativa che li pone a contatto con tale patrimonio. Questi controlli dovranno avvenire nel rispetto delle previsioni

dell'art. 4, comma 1, ma anche del comma 3; b) controlli difensivi in senso stretto, mirati ad accertare selettivamente condotte illecite — anche di aggressione al patrimonio aziendale — di cui si presume, in base ad indizi concreti, siano autori singoli (o alcuni) dipendenti, anche se ciò avviene in occasione dello svolgimento della prestazione lavorativa. In questo caso si tratta di indagini che, salvo quelle condotte direttamente dalle autorità di polizia o dalla magistratura (il che esclude ovviamente l'applicazione dell'art. 4), possono essere attivate dal datore di lavoro avvalendosi di idonei strumenti tecnologici. Questi controlli si collocano al di fuori dell'ambito applicativo dell'art. 4, non avendo ad oggetto l'attività del lavoratore. Peraltro tale impostazione appare perfettamente coerente con l'impostazione data alla tutela dei dati personali dal Regolamento, poiché anche in questo caso la registrazione dei dati e il loro successivo trattamento verrebbe svolto in conformità ai principi di liceità e correttezza in quanto funzionali al contrasto e alla punizione di utilizzi illeciti degli strumenti tecnologici.

Il tema ha trovato soluzioni diverse presso la giurisprudenza di merito italiana pronunciatasi su fattispecie ricadenti nell'ambito di applicazione del nuovo testo dell'art. 4. Mentre secondo alcuni tribunali, conformemente all'opinione appena espressa, la categoria dei controlli difensivi volta ad accertare condotte illecite del dipendente non sarebbe stata assorbita dalla riforma all'interno della norma dello Statuto dei lavoratori (cfr.: T Padova, 22 gennaio 2018, FI; T La Spezia, ord. 25 novembre 2016), secondo un diverso orientamento, il riferimento espresso alla finalità di tutela del patrimonio aziendale, ora contenuto all'interno dell'art. 4, comporta che anche il controllo avente la finalità di accertare la condotta illecita del dipendente debba necessariamente passare attraverso le garanzie predisposte da tale disposizione (cfr. T Roma, ord., 13 giugno 2018, n. 57668).

Il primo orientamento sembra aver trovato una conferma nella soluzione enunciata dalla Camera Grande della Corte EDU nella sentenza 17 ottobre 2019, *López Ribanda e altri c. Spagna*, relativa al caso della installazione da parte di un supermercato di telecamere, non visibili dal personale, in ragione del sospetto di sottrazioni formulato dal manager del supermarket sulla base delle significative perdite economiche registrate nel corso di molti mesi. In tale ipotesi, la Corte EDU ha ritenuto compatibile con l'art. 8 della Convenzione la scelta di installare le telecamere occulte se realizzata contemperando i due interessi concorrenti al rispetto della vita privata dei lavoratori e alla protezione della proprietà privata e della piena operatività dell'organizzazione aziendale del datore. La Corte ha infatti riscontrato come la misura fosse stata adottata nel rispetto del principio di proporzionalità, in quanto limitata rispetto ai luoghi (essendo le telecamere rivolte esclusivamente sulle postazioni di cassa) e ai tempi delle riprese (la durata dell'attività di video sorveglianza era infatti stata limitata al tempo necessario a riscontrare la fondatezza dei sospetti). Inoltre, la Corte ha rilevato che essendo le casse ubicate in un luogo pubblico, l'aspettativa di privacy dei lavoratori dovesse ritenersi necessariamente inferiore rispetto a quelli di altri luoghi privati (come ad es. i bagni o il guardaroba).

**4. Condizioni di legittimità dei controlli a distanza: l'accordo sindacale e l'autorizzazione amministrativa.** Prima di dedicarci ad esaminare in che modo la disciplina posta dall'art. 4 l. n. 300/1970 sia destinata ad interagire con quella dettata dal Codice e dal Regolamento, appare però utile brevemente ricordare che l'art. 4 distingue gli strumenti suscettibili di realizzare un controllo a distanza dell'attività lavorativa in due gruppi, a seconda che per la loro installazione sia imposto o meno il rispetto di un regime di autorizzazione.

Nel primo gruppo devono essere collocati gli strumenti, previsti dal primo comma dell'art. 4, la cui installazione sia avvenuta per far fronte ad **esigenze organizzative e produttive, per la sicurezza del lavoro o per la tutela del patrimonio aziendale**. In tali ipotesi l'installazione è condizionata dalla preventiva sottoscrizione di un **accordo sindacale** che, a differenza di quanto previsto dalla precedente formulazione, può essere stipulato con le RSA o la RSU presenti nell'unità produttiva ovvero con le « associazioni sindacali comparativamente più rappresentative sul piano nazionale » quando i controlli a distanza riguardano « imprese con unità produttive ubicate in diverse province ».

Il legislatore si è così fatto carico del problema — ricorrente nella pratica — delle **aziende plurilocalizzate** che si avvalgono di sistemi di controllo a distanza identici da installare nelle varie unità produttive. La trattativa con le associazioni sindacali esterne, anziché con la RSA/RSU, costituisce un'alternativa facoltativa e non già l'attribuzione di una competenza esclusiva riconosciuta a tali associazioni e sottratta alle rappresentanze sindacali costituite nell'azienda. Si tratta, quindi, di una legittimazione concorrente che implica l'eventualità di un raccordo tra le due strutture sindacali secondo prassi che caratterizzeranno le relazioni sindacali di ogni singola azienda o valutazioni effettuate di volta in volta.

In caso di mancato raggiungimento di un accordo sindacale, l'installazione dello strumento può essere autorizzata dall'Ispettorato territoriale del lavoro competente o dall'Ispettorato nazionale in caso di imprese che abbiano unità produttive ubicate in territori di competenza di ispettorati differenti.

È qui utile precisare che mentre i sindacati potranno del tutto legittimamente richiedere che i dati acquisiti dal datore di lavoro a seguito dei controlli a distanza non siano utilizzabili a fini disciplinari, tale posizione non potrà essere assunta dall'ispettorato del lavoro, nazionale o territoriale, essendo per essi impegnativa la previsione del comma 3 dell'art. 4 per la quale « le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro ».

**5. Le esenzioni riservate agli strumenti utilizzati per rendere la prestazione lavorativa e per la registrazione degli accessi e delle presenze.** Il secondo gruppo di strumenti preso in considerazione dall'art. 4 è costituito da quelli per l'installazione dei quali il datore di lavoro è libero, non essendo necessario che lo stesso acquisisca la preventiva autorizzazione sindacale o amministrativa. Rientrano in tale gruppo gli « strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa » e gli « strumenti di registrazione degli accessi e delle presenze ».

Sottraendo tali strumenti alla necessità della preventiva autorizzazione, il legislatore muove dalla consapevolezza che tali strumenti assolvono alla funzione primaria di consentire al dipendente di rendere la prestazione e, quindi, adempiere agli impegni contrattuali che devono conformarsi all'organizzazione del lavoro come predisposta dall'imprenditore. Ha così ritenuto, in maniera condivisibile, di non poter imporre vincoli potenzialmente interdittivi all'impiego di tali strumenti, dovendo piuttosto occuparsi di tutelare il dipendente per quanto riguarda le « informazioni raccolte » dal datore di lavoro tramite di essi, anche perché tali informazioni sono « utilizzabili a tutti i fini connessi al rapporto di lavoro ». A tale necessità provvede il comma 3 dell'art. 4.

Muovendo da queste premesse, si deve affrontare il nodo problematico relativo all'identificazione degli « **strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa** ».

L'esame deve iniziare dalla relazione intercorrente tra gli « strumenti » del comma 1 e quelli del comma 2 dell'art. 4, per chiarire ciò che li differenzia: le loro caratteristiche morfologiche o piuttosto le finalità del loro impiego? La soluzione corretta appare quest'ultima, come suggerisce l'apertura del comma 2 quando avverte che « la disposizione di cui al comma 1 non si applica [...] »; precisazione necessaria, attesa l'insussistenza di una differenziazione ontologica tra tali « strumenti », per affermare l'inoperatività del comma 1 quando gli stessi « strumenti » siano utilizzati per le finalità del comma 2.

Quindi la distinzione tra comma 1 e 2 dell'art. 4 si coglie guardando alla funzione che gli « strumenti » assolvono nell'organizzazione predisposta dal datore di lavoro e non già alle loro caratteristiche oggettive (su questo tema v. anche le ricostruzioni di ALVINO, 2016, 23; DEL PUNTA, 2016, 99; MAIO, 2016, 1186; MARAZZA, 2016, 9; SALIMBENI, 2015, 601).

Di qui alcune precisazioni.

La prima riguarda il termine « strumenti » che deve intendersi riferito alle due componenti di qualsiasi sistema informatico: l'hardware (dal computer, al tablet, allo smartphone, ecc.) che consente l'accesso ai vari tipi di software e di applicativi che animano il sistema ed il suo funzionamento; senza di essi le apparecchiature resterebbero inerti, anche quanto alla generazione di controlli a distanza. Quindi la riconducibilità degli « strumenti » nel comma 1 o 2 dell'art. 4 deve avvenire in relazione non solo all'hardware, ma anche e prevalentemente al software, quindi ai programmi a cui accede il dipendente.

Da quanto ora accennato discende anche che gli « strumenti » di cui al comma 2 non si possono identificare con gli strumenti di lavoro nel significato più tradizionale del termine, cioè di attrezzi o dotazioni individuali assegnati a ciascun dipendente per lo svolgimento del proprio lavoro. Anzi molto spesso tali strumenti si immedesimano con il/i sistema/i informatico/i di cui l'impresa si è dotata centralmente al quale si connettono i lavoratori utilizzando postazioni (periferiche) fisse o mobili per svolgere le attività di loro competenza.

L'art. 4 comma 2 non pone preclusioni per quanto riguarda gli strumenti informatici utilizzabili dai dipendenti e neppure limiti alla competenza ed alle valutazioni del datore di lavoro che, quindi, restano insindacabili anche in ragione della

maggiore o minore incidenza di tali strumenti sulla riservatezza dei lavoratori (sul punto v. PINTO, *La flessibilità funzionale*, 2016, 348). Infatti il comma 2 dell'art. 4 riguarda tutti gli « strumenti » accomunati dal fatto oggettivo dell'impiego da parte del prestatore a seguito delle decisioni imprenditoriali prese, come già detto, dal datore di lavoro.

Rientrano dunque in maniera pacifica tra gli strumenti di lavoro, ad esempio e per limitarsi agli strumenti oggi indispensabili, la posta elettronica e l'accesso alla rete internet. Con riferimento all'impiego di tali strumenti il Garante ha predisposto nel 2007 (GPDP, provv. 13/2007) delle Linee guida che tuttora costituiscono il punto di riferimento per le imprese circa gli accorgimenti che devono essere adottati per realizzare l'impiego di tali dotazioni compatibilmente con la disciplina posta a protezione dei dati personali del lavoratore.

L'ambito di applicazione del comma 2 dell'art. 4 è contraddistinto anche dal fatto che gli « strumenti » devono servire al dipendente « per rendere la prestazione lavorativa ». Una formulazione ampia all'interno della quale non sembra possibile differenziare gli strumenti allorché siano utilizzati per organizzare oppure per eseguire la prestazione lavorativa, limitando a questi ultimi la previsione dell'art. 4, comma 2 e riconducendo gli altri al comma 1.

Si tratta, infatti, di una distinzione priva di riscontro testuale, in quanto l'art. 4, comma 2, prende in considerazione tutti gli strumenti che a vario titolo concorrono per consentire al lavoratore di « rendere la prestazione lavorativa » e ciò avviene ogni qualvolta lo stesso lavoratore si attiva per dare impulso al loro funzionamento, ma anche quando il dipendente se ne avvale (o vi accede) per acquisire dati utili per rendere tale prestazione.

Le precisazioni fin qui accennate consentono di affrontare una delle casistiche oggi più ricorrenti, quella dei sistemi di geolocalizzazione in uso al dipendente attivabili da un tablet o da uno smartphone; geolocalizzazione che appare opportuno prendere in considerazione anche per dare atto della pluralità di soluzioni prospettabili in relazione ai diversi usi di uno stesso strumento.

Il sistema di **geolocalizzazione** rientra tra gli strumenti previsti dal comma 2 dell'art. 4, quando è utilizzato, ad esempio, da un tecnico tenuto a rendere una prestazione lavorativa che comporta spostamenti da un luogo all'altro a seconda degli interventi da eseguire; interventi che la geolocalizzazione consente di realizzare con maggiore rapidità, segnalando al tecnico il luogo da raggiungere in quel momento più vicino.

In questo caso la geolocalizzazione permette al dipendente di rendere la prestazione lavorativa in tempi più rapidi (ed anche con minor disagio personale limitando gli spostamenti) e ciò costituisce il presupposto dell'applicabilità dell'art. 4, comma 2.

Ad una diversa conclusione si deve giungere quando la prestazione del lavoratore non è caratterizzata da alcuna mobilità territoriale, in questo caso il sistema di geolocalizzazione non è funzionale a rendere tale prestazione e, quindi, potrebbe rientrare nel comma 1 dell'art. 4 (con la conseguenza che sarebbe attivabile solo dopo l'accordo sindacale o l'autorizzazione dell'Ispettorato) sempre che sussista almeno una delle ragioni ivi previste: ad esempio la geolocalizzazione dell'auto

condotta dal dipendente a tutela del bene aziendale (sul tema v. anche circ. INL 7 novembre 2016, n. 2 e GPDP 24 maggio 2017, n. 247).

Fin qui si è detto dei sistemi di geolocalizzazione che realizzano anche un controllo a distanza dell'attività del dipendente, ma potrebbe accadere che **i dati acquisiti non siano accessibili al datore di lavoro** il che esclude l'applicazione dell'art. 4; ad esempio quando il sistema è nella disponibilità della sola compagnia di assicurazione che, a fronte di questa dotazione (cd. *black box*), riduce il costo della polizza. Il collegamento operato dal comma 2 dell'art. 4 tra utilizzo degli « strumenti » e « prestazione lavorativa » consente di affrontare anche la questione relativa a quei **controlli a distanza attivati dal datore di lavoro in adempimento di obblighi posti dalla legge o da una authority** (Consob, Agcom, ecc.) a tutela degli interessi di terzi (ad esempio gli utenti di un servizio). Si tratta di casi, per limitarci solo a qualche riferimento, nei quali si deve procedere alla registrazione del colloquio telefonico nel corso del quale un dipendente raccoglie un ordine di borsa o conclude un contratto di fornitura di servizi con un utente.

In queste ipotesi la registrazione documenta non solo il contratto, ma anche l'operato del dipendente venendo così a configurare un controllo a distanza sull'attività lavorativa che sembra riconducibile nel comma 2 dell'art. 4, proprio perché la prestazione del lavoratore non potrebbe essere resa con una modalità diversa da quella che realizza il controllo a distanza dello stesso dipendente.

C'è poi da aggiungere che, in questo caso, la protezione dell'interesse dell'utente assume, secondo la valutazione espressa dall'ordinamento, carattere cogente e necessario, come tale inconciliabile con la previsione dell'art. 4, comma 1 che sottopone il controllo a distanza alla preventiva autorizzazione sindacale o dell'Ispettorato, non residuando in capo a questi soggetti alcun margine di valutazione in ordine all'attivazione del controllo ed essendo presidiata dal comma 3 (anche con il richiamo al Codice) la tutela dovuta al dipendente quanto alla sua esposizione al controllo.

Sulla scorta di questi spunti si può spostare l'attenzione su un profilo problematico relativo all'applicazione dell'art. 4, comma 2 quando si tratti di **sistemi di sicurezza del lavoro** il cui impiego è monitorato a distanza dal datore di lavoro con inevitabili implicazioni anche sul controllo dell'attività lavorativa.

In prima battuta tali sistemi sembrerebbero rientrare nella previsione del comma 1 dell'art. 4 che espressamente riguarda gli « strumenti » « per la sicurezza del lavoro ». Ma se l'evoluzione tecnologica dovesse evidenziarne la particolare efficacia nel presidio della sicurezza del lavoratore — magari in alcuni contesti produttivi dove i rischi sono più elevati e tali da rendere necessario il potenziamento delle azioni di contrasto — si potrebbe ipotizzare che la sicurezza tecnologica così garantita al dipendente diventi una modalità della prestazione lavorativa obbligatoria *ex art. 2087 c.c.*

Si deve, inoltre, considerare che il comma 1 dell'art. 4 realizza — come in precedenza segnalato — un bilanciamento dei contrapposti interessi, del datore di lavoro al controllo e del dipendente alla riservatezza. Ma tale bilanciamento non può riguardare il caso in esame dove non si pone il tema della tutela degli interessi datoriali all'esercizio del potere di controllo sull'attività lavorativa, bensì quello



dell'obbligo di favorire la sicurezza dei dipendenti nelle forme tecnologicamente più evolute.

In questa prospettiva si potrebbe, quindi, avviare una riflessione sul comma 1 dell'art. 4 per escluderne l'applicazione laddove il controllo a distanza non sia finalizzato a realizzare un interesse del datore di lavoro quale creditore della prestazione lavorativa, quanto piuttosto quello del dipendente assoggettato sì ad un controllo a distanza, ma a tutela della sua sicurezza. Questo primo passaggio consentirebbe, poi, di ricondurre al comma 2 dell'art. 4 (e sempre nel rispetto delle tutele del comma 3) il caso in esame trattandosi di controlli derivanti dall'impiego di strumenti necessari per rendere la prestazione lavorativa, in quanto ne garantirebbero la sicurezza.

Un ultimo cenno sempre relativo all'ambito di applicazione del comma 2 dell'art. 4 riguarda la distinzione tra i controlli a distanza derivanti dall'impiego di software « utilizzati dal lavoratore per rendere la prestazione lavorativa » e l'implementazione di uno di questi software con funzioni aggiuntive, specificamente attivate **per misurare il livello quali-quantitativo della produttività del lavoratore**.

Nel caso in esame i controlli a distanza riconducibili all'art. 4, comma 2 sono quelli che derivano, secondo una non facile indagine tecnica più che giuridica, da un software dotato di varie funzioni sviluppate in modo integrato per lo svolgimento dell'attività lavorativa, ma che realizzano simultaneamente anche un controllo della produttività del singolo dipendente.

Se, invece, quest'ultimo controllo (sulla qualità/efficacia della prestazione) è realizzato da uno sviluppo applicativo originato dallo stesso software che, però, acquisisce una sua autonoma e specifica operatività rispetto alle funzioni di cui si avvale il dipendente per rendere la prestazione lavorativa, il controllo non sarà vietato dall'art. 4 se persegue « esigenze organizzative e produttive » del datore di lavoro, ma richiede il preventivo accordo sindacale o l'autorizzazione dell'Ispettorato essendo riconducibile al comma 1.

Appare più agevole l'identificazione degli « **strumenti di registrazione degli accessi e delle presenze** » a cui si riferisce l'art. 4, comma 2.

Con questa norma il legislatore intende, probabilmente, prendere posizione rispetto ad un orientamento della giurisprudenza — non univoco, ma accolto anche dalla Cassazione (CC, sez. lav., 17 luglio 2007 n. 15892, RGL, 2008, II, 358 ss., nt. BELLAVISTA; CC, sez. lav., 13 maggio 2016 n. 9904, GI, 2016, I, nt. MARAZZA) — che affermava l'applicabilità dell'art. 4 (vecchio testo) al sistema informatizzato di rilevazione delle presenze all'inizio ed alla fine dell'orario di lavoro, in quanto idoneo a realizzare un controllo a distanza sui tempi della prestazione dovuta dal lavoratore, con la conseguenza che l'attivazione di tale sistema avrebbe dovuto essere preceduta dall'accordo sindacale o dell'autorizzazione amministrativa. Cosa che, peraltro, nella pratica avveniva molto raramente.

La norma vigente consente di ritenere superata tale questione equiparando i controlli delle presenze a quelli derivanti dagli strumenti di lavoro per i quali non occorre l'accordo sindacale o l'autorizzazione dell'Ispettorato del lavoro.

Semmai il problema interpretativo si può porre con riferimento al termine « **presenze** », perché il legislatore non precisa se si tratta soltanto di quelle che si

registrano all'entrata ed in uscita e, quindi, lascia aperta la possibilità di un'interpretazione estensiva che consentirebbe l'utilizzo di strumenti in grado di monitorare a distanza la presenza mobile del dipendente anche all'interno dei luoghi di lavoro, vale a dire la mobilità e gli spostamenti effettuati dal lavoratore rispetto alla sua postazione.

Questa interpretazione — seppur letteralmente possibile — non appare però coerente con la *ratio* della norma che accomuna la registrazione degli accessi a quella delle presenze, evidenziando così che si tratta di due situazioni per le quali ricorre la medesima esigenza, cioè quella di acquisire un dato preciso relativo alla posizione del dipendente nel momento dell'accesso o di inizio o fine del lavoro; un dato che, attraverso il controllo, viene fissato nel tempo, tanto è vero che rispetto ad esso il legislatore ne prevede la « registrazione ».

La rilevazione degli accessi può riguardare non soltanto l'ingresso in azienda (allorché si distingue dalla rilevazione dell'inizio dell'orario di servizio), ma anche il controllo di specifiche aree che, all'interno di uno stabilimento, sono riservate soltanto ad alcuni dipendenti, ad esempio per motivi di segretezza delle lavorazioni (oppure di sicurezza) che comportano l'esigenza di monitorare attraverso specifici varchi l'ingresso dei lavoratori.

Ci si potrebbe anche chiedere se il riferimento al controllo degli accessi di cui al comma 2 dell'art. 4, comprenda anche la connessione ai sistemi informatici aziendali.

L'estensione della regola prevista per gli accessi fisici anche a quelli informatici appare possibile sul piano interpretativo, anche se tale questione sembra assorbita e risolta alla stregua della prima parte del comma 2 nel cui ambito è più corretto ricondurre i collegamenti e le connessioni telematiche (ed i controlli a distanza che ne conseguono) effettuati dal dipendente per realizzare la prestazione lavorativa.

**6. Controlli legittimi e utilizzabilità dei dati acquisiti per la gestione del rapporto di lavoro.** Nel comma 3 dell'art. 4 è racchiusa la tutela del dipendente destinata ad operare nella fase in cui, all'esito dei controlli a distanza legittimamente effettuati in conformità ai commi 1 e 2, il datore di lavoro si avvale dei dati acquisiti utilizzandoli « per tutti i fini connessi al rapporto di lavoro ».

A ben vedere, quindi, **la disposizione non riguarda l'esercizio del potere di controllo e le sue modalità, ma una fase successiva** che si colloca a valle del controllo, anzi quando esso si è esaurito, essendo le « informazioni » entrate nella disponibilità del datore di lavoro che potrà utilizzarle, a distanza di tempo o di luogo dal momento della loro acquisizione.

I limiti posti dal legislatore nel comma 3 operano, quindi, con riferimento non esclusivamente al potere di controllo, ma anche alla gestione del rapporto di lavoro ed ai poteri che caratterizzano tale gestione, tra i quali pure quello disciplinare. Ben potendo il datore di lavoro avvalersi delle « informazioni », ad esempio, per valutazioni relative sia alla remunerazione della prestazione lavorativa in rapporto ai risultati raggiunti sia alle competenze professionali del dipendente per il miglior impiego delle energie lavorative.

In altre parole la nuova norma opera un opportuno raccordo tra il potere di controllo tecnologico e gli altri poteri gestionali del datore di lavoro, venendo così a colmare una lacuna del vecchio art. 4 che, com'è noto, alimentava non poche incertezze applicative in ordine all'utilizzabilità dei dati derivanti dal controllo, potendosi ritenere che alla legittimità di tale controllo conseguisse ineluttabilmente la facoltà del datore di lavoro di avvalersene, ma anche, all'opposto che, il limite stabilito dal legislatore del 1970 ai controlli a distanza in funzione di « esigenze organizzative e produttive » o dettate « dalla sicurezza del lavoro » operasse pure con riferimento all'utilizzo dei dati acquisiti.

La questione si può ritenere oggi risolta con il comma 3 dell'art. 4 che incide in termini generali sulla posizione del datore di lavoro ogni qual volta decida di avvalersi dei dati raccolti. **Decisione subordinata al rispetto delle due condizioni** (« [...] a condizione [...] »), **indicate dal legislatore, dalle quali dipende la legittimità del controllo eseguito: a) che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli; b) che i controlli siano eseguiti nel rispetto della disciplina dettata dal d.lgs. n. 196/2003.**

Con riferimento alla seconda delle due condizioni appena indicate, ciò significa che l'**analisi dei dati raccolti** dallo strumento che sia stato legittimamente installato, secondo le regole sopra ricordate, **deve avvenire nel rispetto dei principi generali in materia di trattamento dei dati enunciati dall'art. 5 del regolamento UE 679/2016** (cfr. ALVINO, 2016, 27; DEL PUNTA, 2016, 90; LAMBERTUCCI, 2015, 3).

Le considerazioni accennate sollecitano un duplice chiarimento per quanto concerne i **soggetti destinatari della norma** ed il momento in cui si configura l'utilizzabilità dei dati « a tutti i fini connessi al rapporto di lavoro ».

Non c'è dubbio che il comma 3 dell'art. 4 riguarda il datore di lavoro, ma il suo raggio di azione appare più ampio perché in realtà coinvolge tutti i soggetti a vario titolo competenti in materia di controlli tecnologici a distanza secondo la previsione del comma 1, si tratta: dei sindacati (RSU, RSA, ma anche dei sindacati comparativamente più rappresentativi a livello nazionale), dell'Ispettorato del lavoro (nazionale e territoriale) e dell'Autorità.

È, però, evidente che la norma non vincola i sindacati che ben potranno avanzare richieste per limitare i controlli o i loro effetti e tali richieste formeranno oggetto della trattativa con il datore di lavoro in funzione dell'eventuale accordo di cui al comma 1 (come già segnalato, ciò avverrà sicuramente con riferimento alla non utilizzabilità dei dati a fini disciplinari).

Diversamente si deve dire per l'Ispettorato e per il Garante per i quali la regola posta dal legislatore nel comma 3 dell'art. 4 risulta impegnativa e dovrà conformare il loro operato.

La seconda questione è più complessa e sottile, ma altrettanto rilevante.

Infatti si tratta di capire **quando si configura (cioè dove inizia a porsi) il tema dell'utilizzazione dei dati da parte del datore di lavoro** che potrà avvenire soltanto nel momento in cui si saranno realizzate le condizioni imposte dal legislatore nel comma 3. Ciò significa, in altre parole, tracciare il confine tra l'esercizio del potere di controllo (commi 1 e 2 dell'art. 4) e ciò che si pone a valle di esso.

In questa prospettiva — e riprendendo questioni già accennate — appare possibile far coincidere l'utilizzazione dei dati con l'esame e la valutazione degli stessi da parte del datore di lavoro. Si tratta di un'operazione distinta e distinguibile: infatti essa è prodromica rispetto all'altra relativa ai provvedimenti che saranno adottati dal datore di lavoro, ma è successiva alla raccolta e memorizzazione dei dati.

Seguendo questo ragionamento si potrebbe dire che il datore di lavoro deve ottemperare alle condizioni poste dal comma 3 dell'art. 4 soltanto nel momento in cui decide di procedere all'esame dei dati legittimamente raccolti attraverso il sistema di controllo a distanza. Infatti soltanto dal collegamento tra tali dati ed il singolo lavoratore scaturisce per quest'ultimo la necessità di fruire delle garanzie apprestate dal legislatore.

**Ne consegue che il datore di lavoro è tenuto ad ottemperare alle condizioni poste dal comma 3 dell'art. 4 allorché procede ad analizzare e valutare i dati raccolti** che, pur essendo nella sua disponibilità, solo in questo caso verranno evidenziati nel loro collegamento con la prestazione del singolo lavoratore, identificandosi in ciò il primo atto di utilizzo dei dati.

Riprendendo quanto già detto, la raccolta dei dati (cioè l'esercizio del potere di controllo del datore di lavoro) dovrà avvenire nel rispetto del comma 1 dell'art. 4 (quindi previo accordo sindacale o autorizzazione dell'Ispettorato, salvi i casi riconducibili nel comma 2) a tutela della riservatezza della generalità dei lavoratori, mentre l'utilizzo dei dati postula l'« adeguata informazione » a protezione della posizione dei dipendenti che assume rilievo nel momento in cui il datore di lavoro decide di avvalersi di tali dati.

È necessario precisare che tale decisione non potrà riguardare ad personam un singolo dipendente, ma dovrà realizzarsi per tutti i dati acquisiti nei confronti dei lavoratori sottoposti al medesimo sistema di controllo a distanza, proprio perché in tal modo i dati vengono associati alla persona del prestatore di lavoro.

Sul piano applicativo le considerazioni svolte inducono ad ipotizzare la possibilità di un diverso approccio del datore di lavoro all'obbligo dell'« adeguata informazione » nei confronti del personale dipendente che in alcune occasioni (ad esempio per quanto attiene alla rilevazione delle presenze) sarà necessitata dall'utilizzazione routinaria di queste informazioni, mentre in altri casi avverrà se e quando il datore di lavoro intenderà avviare un esame dei dati raccolti, ma, beninteso, prima che tale esame venga esperito. Naturalmente l'ipotesi a cui si è accennato potrà porsi in concreto soltanto per quei dati che siano distinguibili e separabili, consentendo l'esame di alcuni di essi e non di altri.

**7. L'informazione trasparente al lavoratore come condizione per l'utilizzabilità dei dati raccolti dal datore di lavoro.** La ricostruzione del dato normativo fin qui accennata nei suoi tratti essenziali, porta a ritenere che l'informazione dovuta dal datore di lavoro ex art. 4, comma 3 realizza una **tutela della persona del dipendente fondata sulla trasparenza**. Ciò nella convinzione che l'obbligo di rendere edotto il lavoratore in ordine ai controlli a cui è sottoposto costituisce la modalità più efficace per proteggerlo non dal controllo, già avvenuto nel rispetto

dei limiti previsti dal legislatore (commi 1 e 2 dell'art. 4), ma dall'utilizzo dei dati per le potenziali ripercussioni sulla posizione del prestatore nell'ambito del rapporto di lavoro (per quanto riguarda i profili disciplinari, ma non soltanto questi). Ciò sta a significare che l'interesse del lavoratore in tal modo salvaguardato dal legislatore non è quello alla riservatezza il cui presidio è affidato, come più sopra messo in rilievo, ai principi generali sanciti dal Regolamento e dal Codice ed al bilanciamento con il potere datoriale di controllo realizzato dai commi 1 e 2 dell'art. 4, ma quello alla **verificabilità del corretto procedimento di trattamento dei dati**.

Infatti, l'adeguata informazione imposta dal comma 3 dell'art. 4 implica la trasparente rappresentazione di tutto l'iter che va dalle modalità d'uso dello strumento di cui si avvale il dipendente alla raccolta dei dati relativi alla prestazione lavorativa. Ciò dovrebbe consentire al lavoratore di evidenziare errori o manipolazioni delle informazioni che il datore di lavoro intende utilizzare, acquisendo elementi per difendersi di fronte a tali controlli, proprio perché esercitati con modalità palesi e non occulte.

Tale prospettiva dà quindi ragione della natura speciale dell'art. 4 rispetto all'ambito oggetto di regolazione da parte del Regolamento. Specialità che comunque permette di riscontrare la convergenza sul valore di fondo delle due discipline identificabile nell'obbligo di informazione funzionale alla piena realizzazione anche dei principi in materia di protezione dei dati personali.

Il divieto di controlli occulti sulla prestazione lavorativa costituisce, quindi, il principio guida che accomuna nello Statuto dei lavoratori i controlli disciplinati dall'art. 3 con quelli dell'art. 4.

A questo punto ci si deve chiedere quali siano le modalità dell'« adeguata informazione » da rendere al lavoratore.

Partendo dalla scontata considerazione che l'informativa, proprio perché è tale, non richiede alcuna accettazione dei lavoratori che ne sono destinatari, le questioni che si pongono riguardano almeno due profili: il contenuto dell'informativa e le modalità con le quali la stessa deve essere portata a conoscenza del personale dipendente.

Quanto all'adeguatezza del suo **contenuto** i due riferimenti forniti dal legislatore — le « modalità d'uso degli strumenti » e l'« effettuazione dei controlli » — sembrano costituire un'endiadi utilizzata dal legislatore per chiarire le finalità stesse dell'informativa e, così, individuarne il contenuto necessario. I due riferimenti, quindi, devono essere considerati in modo concorrente e coordinato, nel senso che le modalità d'uso — delle quali occorre dare conto nell'informativa — sono quelle da cui consegue il controllo, cioè l'acquisizione dei dati relativi alla prestazione lavorativa del dipendente. Non si tratta, quindi, di redigere un manualetto di istruzioni per l'impiego dello strumento, ma di identificare le modalità del suo utilizzo che comportano l'acquisizione di dati relativi al lavoratore. In poche parole, spiegare come l'uso dello strumento si raccorda con il controllo che ne deriva.

La quantità delle informazioni da trasmettere al lavoratore non dovrà essere eccessiva, perché costituisce un dato di comune esperienza che la sovrabbondanza non favorisce la conoscibilità e la comprensione delle stesse informazioni che, anzi, richiedono un'esposizione completa, ma sintetica.

Proprio per questo appare preferibile un'informazione mirata e non generalizzata, nel senso che tale informazione dovrà riguardare gli strumenti utilizzati (o utilizzabili) dal lavoratore che così vengono ad essere identificati con riferimento ai controlli cui è sottoposto ciascun dipendente (o gruppi di lavoratori che utilizzano gli stessi strumenti). Invece un'informativa rivolta alla generalità dei dipendenti e che riguardi complessivamente tutti gli strumenti impiegati nell'azienda potrebbe risultare non coerente con la finalità perseguita dal legislatore di consentire la puntuale conoscenza da parte del lavoratore dei controlli ai quali è assoggettato. Quanto appena detto consente di passare al secondo punto, cioè le **modalità con le quali l'informativa deve essere portata a conoscenza dei lavoratori** con la consapevolezza della mancanza di un'indicazione espressa da parte del legislatore. Per risolvere il quesito, e quindi comprendere le modalità della sua comunicazione (pubblicità), occorre partire dal contenuto dell'informazione. Se quest'ultimo non è generalizzabile per tutto il personale dipendente, in quanto gli strumenti impiegati dai lavoratori sono differenziati, **i destinatari di essa saranno soltanto quei dipendenti che si avvalgono di determinati strumenti**, ma non gli altri che impiegano strumenti diversi; l'estensione a questi ultimi dell'informativa dovuta ai primi potrebbe, addirittura, generare confusione.

Alla questione ora esaminata si aggiunge l'altra che riguarda la **prova** che il datore di lavoro dovrà fornire, in caso di contestazione in sede giudiziaria, in ordine all'adempimento degli obblighi di informazione di cui è gravato. In questo caso la ricevuta della comunicazione effettuata nei confronti di ciascun lavoratore costituisce la prova documentale più sicura, anche se la trasmissione è stata effettuata in via telematica (con una e-mail o mediante lettura sul sito aziendale debitamente documentata). Ciò, però, non esclude che la prova possa essere fornita anche con riferimento a modalità diverse di comunicazione, ad esempio, mediante affissione in luoghi accessibili ai lavoratori interessati.

**8. Tutela della riservatezza del lavoratore e del datore di lavoro nel telelavoro, nel lavoro agile e nel lavoro domestico.** Il d.lgs. n. 101/2018 ha solo marginalmente toccato l'art. 115, inserendo al suo interno il riferimento al lavoro agile, previsto e regolamentato dagli artt. 18 ss. l. n. 81/2017.

Il lavoro agile, come il telelavoro, si caratterizza per il fatto che la prestazione lavorativa è, nella maggior parte dei casi, svolta dal lavoratore avvalendosi di strumenti tecnologici che consentono il collegamento a distanza con il datore di lavoro (per la distinzione tra telelavoro e lavoro agile v.: SANTORO PASSARELLI G., 2017, 7; GAETA, 2015, 1; PINTO, *La flessibilità funzionale*, 2016, 345; TIRABOSCHI, 2017, 1). Ne consegue che la disposizione in parola assolve la funzione di riaffermare — ancorché non ve ne fosse bisogno sul piano delle regole che sarebbero state comunque applicabili a questa modalità di svolgimento del rapporto di lavoro — che l'impiego di tali strumenti deve avvenire nel rispetto di tutti quei principi e regole che sono posti a presidio della personalità e della libertà morale del lavoratore.

Troveranno dunque applicazione anche al telelavoro, al lavoro agile e al lavoro domestico tutte le norme sin qui esaminate finalizzate a evitare il controllo a distanza dell'attività lavorativa.

## INDICE SISTEMATICO

### DISCIPLINA INTERNAZIONALE

#### Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali

- Art. 8** *Diritto al rispetto della vita privata e familiare*. . . . . 3  
(MARINA CASTELLANETA)

### DISCIPLINA EUROPEA

#### Carta dei diritti fondamentali dell'Unione Europea

- Art. 7** *Rispetto della vita privata e della vita familiare*. . . . . 17  
(GIUSEPPE MARTINICO)
- Art. 8** *Protezione dei dati di carattere personale*. . . . . 35  
(ORESTE POLLICINO (§§ 5, 6) e MARCO BASSINI (§§ 1-3, 4, 6))

#### Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati - GDPR)

- Art. 1** *Oggetto e finalità*. . . . . 113  
(GIUSELLA FINOCCHIARO)
- Art. 2** *Ambito di applicazione materiale*. . . . . 129  
(MICHELE GRAZIADEI)
- Art. 3** *Ambito di applicazione territoriale*. . . . . 143  
(MARIAVITTORIA CATANZARITI)
- Art. 4** *Definizioni*. . . . . 153  
(ALBERTO DE FRANCESCHI)
- Art. 5** *Principi applicabili al trattamento di dati personali*. . . . . 176  
(GIANCLAUDIO MALGIERI)
- Art. 6** *Liceità del trattamento*. . . . . 191  
(DIANORA POLETTI)
- Art. 7** *Condizioni per il consenso*. . . . . 205  
(FAUSTO CAGGIA)
- Art. 8** *Condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione*. . . . . 228  
(CLAUDIA MORGANA CASCIONE)

INDICE SISTEMATICO

<b>Art. 9</b> <i>Trattamento di categorie particolari di dati personali</i> .....	239
I. <i>Profili generali</i> (ARIANNA THIENE) .....	240
II. <i>Il trattamento dei dati particolari: il dato genetico</i> (LUCIA SCAFFARDI) .....	249
<b>Art. 10</b> <i>Trattamento dei dati personali relativi a condanne penali e reati</i> .....	262
(MARCO BASSINI)	
<b>Art. 11</b> <i>Trattamento che non richiede l'identificazione</i> .....	270
(ENZA PELLECCCHIA)	
<b>Art. 12</b> <i>Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato</i> .....	276
(AMARILLIDE GENOVESE)	
<b>Art. 13</b> <i>Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato</i>	
<b>Art. 14</b> <i>Informazioni da fornire qualora i dati personali non siano stati ottenuti dall'interessato</i> .....	288
(LAURA LIGUORI)	
<b>Art. 15</b> <i>Diritto di accesso dell'interessato</i> .....	304
(ALBERTO MARIA GAMBINO (§§ 1, 3, 4, 5) e MATTEO SIRAGUSA (§§ 2, 6, 7, 8))	
<b>Art. 16</b> <i>Diritto di rettifica</i> .....	316
(SIMONE GIANELLO)	
<b>Art. 17</b> <i>Diritto alla cancellazione ("diritto all'oblio")</i> .....	325
(GIUSELLA FINOCCHIARO)	
<b>Art. 18</b> <i>Diritto alla limitazione di trattamento</i> .....	336
(GIORGIO GIANNONE CODIGLIONE)	
<b>Art. 19</b> <i>Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento</i> .....	342
(GIORGIO GIANNONE CODIGLIONE)	
<b>Art. 20</b> <i>Diritto alla portabilità dei dati</i> .....	348
(VALERIA FALCE)	
<b>Art. 21</b> <i>Diritto di opposizione</i> .....	366
(GIOVANNI COMANDÉ)	
<b>Art. 22</b> <i>Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione</i> .....	378
(FRANCESCA LAGIOIA, GIOVANNI SARTOR, ANDREA SIMONCINI)	
<b>Art. 23</b> <i>Limitazioni</i> .....	390
(MARINA CAPORALE)	
<b>Art. 24</b> <i>Responsabilità del titolare del trattamento</i> .....	398
(FRANCESCO PIZZETTI (§§ 1 e 6) e LAURA GRECO (§§ da 2 a 5))	
<b>Art. 25</b> <i>Protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita</i> .....	410
(MATILDE RATTI)	
<b>Art. 26</b> <i>Contitolari del trattamento</i> .....	422
(FRANCESCO PIZZETTI (§§ 1, 2 e 2.1) e LAURA GRECO (§§ da 2.2 a 4))	



<b>Art. 27</b> <i>Rappresentanti di titolari del trattamento o dei responsabili del trattamento non stabiliti nell'Unione</i> . . . . .	449
(FABIO BRAVO)	
<b>Art. 28</b> <i>Responsabile del trattamento</i> . . . . .	456
(FRANCESCO PIZZETTI (§§ 1 e 5) e LAURA GRECO (§§ da 2 a 4.1))	
<b>Art. 29</b> <i>Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento</i> . . . . .	478
(FABIO BRAVO)	
<b>Art. 30</b> <i>Registri delle attività di trattamento</i> . . . . .	488
(CARLO ROSSI CHAUVENET)	
<b>Art. 31</b> <i>Cooperazione con l'autorità di controllo</i> . . . . .	496
(FABIO BRAVO)	
<b>Art. 32</b> <i>Sicurezza del trattamento</i> . . . . .	502
(MARIA SAMANTHA ESPOSITO)	
<b>Art. 33</b> <i>Notifica di una violazione dei dati personali all'autorità di controllo</i> . . . . .	514
(GIUSEPPE VACIAGO)	
<b>Art. 34</b> <i>Comunicazione di una violazione dei dati personali all'interessato</i> . . . . .	524
(GIUSEPPE VACIAGO)	
<b>Art. 35</b> <i>Valutazione d'impatto sulla protezione dei dati</i> . . . . .	530
(ALESSANDRO MANTELERO)	
<b>Art. 36</b> <i>Consultazione preventiva</i> . . . . .	553
(ALESSANDRO MANTELERO)	
<b>Art. 37</b> <i>Designazione del responsabile della protezione dei dati</i> . . . . .	557
(MARCO BASSINI)	
<b>Art. 38</b> <i>Posizione del responsabile della protezione dei dati</i> . . . . .	573
(MARCO BASSINI)	
<b>Art. 39</b> <i>Compiti del responsabile della protezione dei dati</i> . . . . .	579
(MARCO BASSINI)	
<b>Art. 40</b> <i>Codici di condotta</i>	
<b>Art. 41</b> <i>Controllo dei codici di condotta approvati</i> . . . . .	586
(SERENA SILEONI)	
<b>Art. 42</b> <i>Certificazione</i>	
<b>Art. 43</b> <i>Organismi di certificazione</i> . . . . .	603
(GIOVANNI MARIA RICCIO)	
<b>Art. 44</b> <i>Principio generale per il trasferimento</i> . . . . .	616
(PAOLA PIRODDI)	
<b>Art. 45</b> <i>Trasferimento sulla base di una decisione di adeguatezza</i> . . . . .	628
(PAOLA PIRODDI)	
<b>Art. 46</b> <i>Trasferimento soggetto a garanzie adeguate</i> . . . . .	640
(PAOLA PIRODDI)	

<b>Art. 47</b> <i>Norme vincolanti d'impresa</i> . . . . .	651
(FRANCESCA GALLI)	
<b>Art. 48</b> <i>Trasferimento o comunicazione non autorizzati dal diritto dell'Unione</i> . . . . .	662
(FRANCESCA GALLI)	
<b>Art. 49</b> <i>Deroghe in specifiche situazioni.</i> . . . . .	671
(FRANCESCA GALLI)	
<b>Art. 50</b> <i>Cooperazione internazionale per la protezione dei dati personali.</i> . . . . .	680
(MARIO CARTA)	
<b>Art. 51</b> <i>Autorità di controllo.</i> . . . . .	693
(FRANCESCO CARDARELLI)	
<b>Art. 52</b> <i>Indipendenza</i>	
<b>Art. 53</b> <i>Condizioni generali per i membri dell'autorità di controllo</i>	
<b>Art. 54</b> <i>Norme sull'istituzione dell'autorità di controllo</i> . . . . .	707
(FRANCESCO CARDARELLI)	
<b>Art. 55</b> <i>Competenza.</i> . . . . .	726
(FRANCESCO CARDARELLI)	
<b>Art. 56</b> <i>Competenza dell'autorità di controllo capofila.</i> . . . . .	731
(FRANCESCO CARDARELLI)	
<b>Art. 57</b> <i>Compiti</i>	
<b>Art. 58</b> <i>Poteri</i> . . . . .	741
(FRANCESCO CARDARELLI)	
<b>Art. 59</b> <i>Relazioni di attività</i> . . . . .	752
(FRANCESCO CARDARELLI)	
<b>Art. 60</b> <i>Cooperazione tra l'autorità di controllo capofila e le altre autorità di controllo interessate</i>	
<b>Art. 61</b> <i>Assistenza reciproca</i>	
<b>Art. 62</b> <i>Operazioni congiunte delle autorità di controllo.</i> . . . . .	756
(FRANCESCO CARDARELLI)	
<b>Art. 63</b> <i>Meccanismo di coerenza.</i> . . . . .	766
(FEDERICO LUBIAN)	
<b>Art. 64</b> <i>Parere del comitato europeo per la protezione dei dati.</i> . . . . .	776
(FEDERICO LUBIAN)	
<b>Art. 65</b> <i>Composizione delle controversie da parte del comitato.</i> . . . . .	791
(FEDERICO LUBIAN)	
<b>Art. 66</b> <i>Procedura d'urgenza.</i> . . . . .	806
(FEDERICO LUBIAN)	
<b>Art. 67</b> <i>Scambio di informazioni.</i> . . . . .	811
(FEDERICO LUBIAN)	
<b>Art. 68</b> <i>Comitato europeo per la protezione dei dati.</i> . . . . .	818
(GABRIELE DELLA MORTE)	

<b>Art. 69</b> <i>Indipendenza</i> .....	823
(GABRIELE DELLA MORTE)	
<b>Art. 70</b> <i>Compiti del comitato</i> .....	827
(GABRIELE DELLA MORTE)	
<b>Art. 71</b> <i>Relazioni</i> .....	834
(GABRIELE DELLA MORTE)	
<b>Art. 72</b> <i>Procedura</i> .....	838
(GABRIELE DELLA MORTE)	
<b>Art. 73</b> <i>Presidente</i> .....	840
(GABRIELE DELLA MORTE)	
<b>Art. 74</b> <i>Compiti del Presidente</i> .....	842
(GABRIELE DELLA MORTE)	
<b>Art. 75</b> <i>Segreteria</i> .....	844
(GABRIELE DELLA MORTE)	
<b>Art. 76</b> <i>Riservatezza</i> .....	847
(GABRIELE DELLA MORTE)	
<b>Art. 77</b> <i>Diritto di proporre reclamo all'autorità di controllo</i> .....	850
(GIOVANNI GUERRA)	
<b>Art. 78</b> <i>Diritto a un ricorso giurisdizionale effettivo nei confronti dell'autorità di controllo.</i>	
<b>Art. 79</b> <i>Diritto a un ricorso giurisdizionale effettivo nei confronti del titolare del trattamento o del responsabile del trattamento</i> .....	857
(FEDERICA RESTA)	
<b>Art. 80</b> <i>Rappresentanza degli interessati</i> .....	872
(PAOLA CHIARA RUGGIERI)	
<b>Art. 81</b> <i>Sospensione delle azioni</i> .....	880
(PAOLA CHIARA RUGGIERI)	
<b>Art. 82</b> <i>Diritto al risarcimento e responsabilità</i> .....	886
(SALVATORE SICA)	
<b>Art. 83</b> <i>Condizioni generali per infliggere sanzioni amministrative pecuniarie</i> .....	894
(MARCO BASSINI)	
<b>Art. 84</b> <i>Sanzioni</i> .....	906
(MARCO BASSINI)	
<b>Art. 85</b> <i>Trattamento e libertà d'espressione e di informazione</i> .....	912
(ROBERTO D'ORAZIO)	
<b>Art. 86</b> <i>Trattamento e accesso del pubblico ai documenti ufficiali</i> .....	937
(MARINA CAPORALE)	
<b>Art. 87</b> <i>Trattamento del numero di identificazione nazionale</i> .....	943
(MARINA CAPORALE)	
<b>Art. 88</b> <i>Trattamento dei dati nell'ambito dei rapporti di lavoro</i> .....	947
(SILVIA GIUCCIOVINO)	

INDICE SISTEMATICO

<b>Art. 89</b>	<i>Garanzie e deroghe relative al trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici. . . . .</i>	957
	(ROSSANA DUCATO)	
<b>Art. 90</b>	<i>Obblighi di segretezza. . . . .</i>	975
	(MARIAVITTORIA CATANZARITI)	
<b>Art. 91</b>	<i>Norme di protezione dei dati vigenti presso chiese e associazioni religiose. . . . .</i>	981
	(MICHELE PORCELLUZZI)	
<b>Art. 92</b>	<i>Esercizio della delega</i>	
<b>Art. 93</b>	<i>Procedura di comitato</i>	
<b>Art. 94</b>	<i>Abrogazione della direttiva 95/46/CE</i>	
<b>Art. 95</b>	<i>Rapporto con la direttiva 2002/58/CE</i>	
<b>Art. 96</b>	<i>Rapporto con accordi precedentemente conclusi</i>	
<b>Art. 97</b>	<i>Relazioni della Commissione</i>	
<b>Art. 98</b>	<i>Riesame di altri atti legislativi dell'Unione in materia di protezione dei dati</i>	
<b>Art. 99</b>	<i>Entrata in vigore e applicazione. . . . .</i>	991

DISCIPLINA NAZIONALE

**D.lgs. 30 giugno 2003, n. 196. — Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Codice della Privacy)**

<b>Art. 1</b>	<i>Oggetto . . . . .</i>	995
	(GUIDO ALPA)	
<b>Art. 2</b>	<i>Finalità . . . . .</i>	1008
	(GIUSELLA FINOCCHIARO)	
<b>Art. 2-bis</b>	<i>Autorità di controllo . . . . .</i>	1009
	(GIOVANNI GUERRA)	
<b>Art. 2-ter</b>	<i>Base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri . . . . .</i>	1011
	(FRANCESCO CARDARELLI)	
<b>Art. 2-quater</b>	<i>Regole deontologiche . . . . .</i>	1024
	(ROBERTO D'ORAZIO)	
<b>Art. 2-quinquies</b>	<i>Consenso del minore in relazione ai servizi della società dell'informazione. . . . .</i>	1035
	(CLAUDIA MORGANA CASCIONE)	
<b>Art. 2-sexies</b>	<i>Trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante . . . . .</i>	1043
	(FULVIO CORTESE)	

INDICE SISTEMATICO

*Art. 2-septies* Misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute . . . . . 957  
 (FRANCESCA ZANOVELLO)

*Art. 2-octies* Principi relativi al trattamento di dati relativi a condanne penali e reati . . . 975  
 (GIULIO ERRANI)

*Art. 2-nonies* Trattamenti disciplinati dalla Presidenza della Repubblica, dalla Camera dei deputati, dal Senato della Repubblica e dalla Corte costituzionale . . . . . 981  
 (ROBERTO D'ORAZIO)

*Art. 2-decies* Inutilizzabilità dei dati . . . . . 987  
 (ELENA D'ALESSANDRO)

*Art. 2-undecies* Limitazioni ai diritti dell'interessato  
*Art. 2-duodecies* Limitazioni per ragioni di giustizia . . . . . 1103  
 (LICIA CALIFANO)

*Art. 2-terdecies* Diritti riguardanti le persone decedute . . . . . 1115  
 (GIORGIO RESTA)

*Art. 2-quaterdecies* Attribuzione di funzioni e compiti a soggetti designati . . . . . 1125  
 (FABIO BRAVO)

*Art. 2-quinquiesdecies* Trattamento che presenta rischi elevati per l'esecuzione di un compito di interesse pubblico . . . . . 1143  
 (ALESSANDRO MANTELERO)

*Art. 2-sexiesdecies* Responsabile della protezione dei dati per i trattamenti effettuati dalle autorità giudiziarie nell'esercizio delle loro funzioni . . . . . 1144  
 (FRANCESCO CRISAFULLI)

*Art. 2-septiesdecies* Organismo nazionale di accreditamento . . . . . 1153  
 (FABIO BRAVO)

*Artt. 3-6* [Abrogati] . . . . . 1169  
*Artt. 7-10* [Abrogati] . . . . . 1169  
*Artt. 11-17* [Abrogati] . . . . . 1170  
*Artt. 18-22* [Abrogati] . . . . . 1170  
*Artt. 23-27* [Abrogati] . . . . . 1170  
*Artt. 28-30* [Abrogati] . . . . . 1170  
*Artt. 31-32-bis* [Abrogati] . . . . . 1171  
*Artt. 33-36* [Abrogati] . . . . . 1171  
*Artt. 37-41* [Abrogati] . . . . . 1171  
*Artt. 42-45* [Abrogati] . . . . . 1171

*Art. 45-bis* Base giuridica . . . . . 1172  
 (MARINA CAPORALE)

*Artt. 46-49* [Abrogati] . . . . . 1175

*Art. 50* Notizie o immagini relative a minori . . . . . 1175  
 (ROSANNA DE MEO)

*Art. 2-septies* Misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute . . . . . 1050  
 (FRANCESCA ZANOVELLO)

*Art. 2-octies* Principi relativi al trattamento di dati relativi a condanne penali e reati . . . 1062  
 (GIULIO ERRANI)

*Art. 2-nonies* Trattamenti disciplinati dalla Presidenza della Repubblica, dalla Camera dei deputati, dal Senato della Repubblica e dalla Corte costituzionale . . . . . 1078  
 (ROBERTO D'ORAZIO)

*Art. 2-decies* Inutilizzabilità dei dati . . . . . 1087  
 (ELENA D'ALESSANDRO)

*Art. 2-undecies* Limitazioni ai diritti dell'interessato  
*Art. 2-duodecies* Limitazioni per ragioni di giustizia . . . . . 1103  
 (LICIA CALIFANO)

*Art. 2-terdecies* Diritti riguardanti le persone decedute . . . . . 1115  
 (GIORGIO RESTA)

*Art. 2-quaterdecies* Attribuzione di funzioni e compiti a soggetti designati . . . . . 1125  
 (FABIO BRAVO)

*Art. 2-quinquiesdecies* Trattamento che presenta rischi elevati per l'esecuzione di un compito di interesse pubblico . . . . . 1143  
 (ALESSANDRO MANTELERO)

*Art. 2-sexiesdecies* Responsabile della protezione dei dati per i trattamenti effettuati dalle autorità giudiziarie nell'esercizio delle loro funzioni . . . . . 1144  
 (FRANCESCO CRISAFULLI)

*Art. 2-septiesdecies* Organismo nazionale di accreditamento . . . . . 1153  
 (FABIO BRAVO)

*Artt. 3-6* [Abrogati] . . . . . 1169  
*Artt. 7-10* [Abrogati] . . . . . 1169  
*Artt. 11-17* [Abrogati] . . . . . 1170  
*Artt. 18-22* [Abrogati] . . . . . 1170  
*Artt. 23-27* [Abrogati] . . . . . 1170  
*Artt. 28-30* [Abrogati] . . . . . 1170  
*Artt. 31-32-bis* [Abrogati] . . . . . 1171  
*Artt. 33-36* [Abrogati] . . . . . 1171  
*Artt. 37-41* [Abrogati] . . . . . 1171  
*Artt. 42-45* [Abrogati] . . . . . 1171

*Art. 45-bis* Base giuridica . . . . . 1172  
 (MARINA CAPORALE)

*Artt. 46-49* [Abrogati] . . . . . 1175

*Art. 50* Notizie o immagini relative a minori . . . . . 1175  
 (ROSANNA DE MEO)

<p><b>Art. 51</b> <i>Principi generali</i>. . . . . (PIEREMILIO SAMMARCO)</p> <p><b>Art. 52</b> <i>Dati identificativi degli interessati</i>. . . . . (PIEREMILIO SAMMARCO)</p> <p><b>Artt. 53-56</b> [Abrogati]. . . . .</p> <p><b>Art. 57</b> <i>Disposizioni di attuazione</i>. . . . . (FEDERICA RESTA)</p> <p><b>Art. 58</b> <i>Trattamenti di dati personali per fini di sicurezza nazionale o difesa</i>. . . . . (FEDERICA RESTA)</p> <p><b>Art. 59</b> <i>Accesso a documenti amministrativi e accesso civico</i></p> <p><b>Art. 60</b> <i>Dati relativi alla salute o alla vita sessuale o all'orientamento sessuale</i> . . . . . (CARLO COLAPIETRO)</p> <p><b>Art. 61</b> <i>Utilizzazione di dati pubblici e regole deontologiche</i> . . . . . (PAOLO GUARDA)</p> <p><b>Artt. 62-63</b> [Abrogati]. . . . .</p> <p><b>Artt. 64-73</b> [Abrogati]. . . . .</p> <p><b>Art. 74</b> [Contrassegni su veicoli e accessi a centri storici] . . . . .</p> <p><b>Art. 75</b> <i>Specifiche condizioni in ambito sanitario</i>. . . . . (MAURIZIO DI MASI)</p> <p><b>Art. 76</b> [Esercenti professioni sanitarie e organismi sanitari pubblici] . . . . .</p> <p><b>Art. 77</b> <i>Modalità particolari</i>. . . . . (MAURIZIO DI MASI)</p> <p><b>Art. 78</b> <i>Informazioni del medico di medicina generale o del pediatra</i> . . . . . (MAURIZIO DI MASI)</p> <p><b>Art. 79</b> <i>Informazioni da parte di strutture pubbliche e private che erogano prestazioni sanitarie e socio-sanitarie</i> . . . . . (MAURIZIO DI MASI)</p> <p><b>Art. 80</b> <i>Informazioni da parte di altri soggetti</i>. . . . . (MAURIZIO DI MASI)</p> <p><b>Art. 81</b> [Prestazione del consenso]. . . . .</p> <p><b>Art. 82</b> <i>Emergenze e tutela della salute e dell'incolumità fisica</i> . . . . . (MAURIZIO DI MASI)</p> <p><b>Artt. 83-84</b> [Abrogati]. . . . .</p> <p><b>Artt. 85-86</b> [Abrogati]. . . . .</p> <p><b>Artt. 87-89</b> [Abrogati]. . . . .</p> <p><b>Art. 89-bis</b> <i>Prescrizioni di medicinali</i>. . . . . (FEDERICA GIOVANELLA)</p> <p><b>Art. 90</b> [Trattamento dei dati genetici e donatori di midollo osseo]. . . . .</p> <p><b>Art. 91</b> [Dati trattati mediante carte]. . . . .</p>	<p>1182</p> <p>1185</p> <p>1192</p> <p>1192</p> <p>1204</p> <p>1209</p> <p>1228</p> <p>1232</p> <p>1233</p> <p>1233</p> <p>1233</p> <p>1233</p> <p>1243</p> <p>1243</p> <p>1251</p> <p>1262</p> <p>1268</p> <p>1274</p> <p>1274</p> <p>1279</p> <p>1280</p> <p>1280</p> <p>1280</p> <p>1284</p> <p>1284</p>
--	---

INDICE SISTEMATICO

<b>Art. 92</b> <i>Cartelle cliniche</i> . . . . .	1284
(FEDERICA GIOVANELLA)	
<b>Art. 93</b> <i>Certificato di assistenza al parto</i> . . . . .	1290
(FEDERICA GIOVANELLA)	
<b>Art. 94</b> [ <i>Banche di dati, registri e schedari in ambito sanitario</i> ] . . . . .	1295
<b>Art. 95</b> [ <i>Dati sensibili e giudiziari</i> ] . . . . .	1296
<b>Art. 96</b> <i>Trattamento di dati relativi a studenti</i> . . . . .	1296
(EDOARDO RUZZI)	
<b>Art. 97</b> <i>Ambito applicativo</i> . . . . .	1307
(FEDERICA GIOVANELLA)	
<b>Art. 98</b> [ <i>Finalità di rilevante interesse pubblico</i> ] . . . . .	1309
<b>Art. 99</b> <i>Durata del trattamento</i> . . . . .	1309
(FEDERICA GIOVANELLA)	
<b>Art. 100</b> <i>Dati relativi ad attività di studio e ricerca</i> . . . . .	1313
(FEDERICA GIOVANELLA)	
<b>Art. 101</b> <i>Modalità di trattamento</i> . . . . .	1317
(ROBERTO D'ORAZIO)	
<b>Art. 102</b> <i>Regole deontologiche per il trattamento a fini di archiviazione nel pubblico interesse o di ricerca storica</i> . . . . .	1326
(ROBERTO D'ORAZIO)	
<b>Art. 103</b> <i>Consultazione di documenti conservati in archivi</i> . . . . .	1335
(ROBERTO D'ORAZIO)	
<b>Art. 104</b> <i>Ambito applicativo e dati identificativi a fini statistici o di ricerca scientifica</i> . . . . .	1345
(ROSSANA DUCATO)	
<b>Art. 105</b> <i>Modalità di trattamento</i> . . . . .	1348 *
(ROSSANA DUCATO)	
<b>Art. 106</b> <i>Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica</i> . . . . .	1356 *
(ROSSANA DUCATO)	
<b>Art. 107</b> <i>Trattamento di categorie particolari di dati personali</i> . . . . .	1360 **
(ROSSANA DUCATO)	
<b>Art. 108</b> <i>Sistema statistico nazionale</i> . . . . .	1362
(ROSSANA DUCATO)	
<b>Art. 109</b> <i>Dati statistici relativi all'evento nascita</i> . . . . .	1367
(ROSSANA DUCATO)	
<b>Art. 110</b> <i>Ricerca medica, biomedica ed epidemiologica</i> . . . . .	1369
(PAOLO GUARDA)	
<b>Art. 110-bis</b> <i>Trattamento ulteriore da parte di terzi dei dati personali a fini di ricerca scientifica o a fini statistici</i> . . . . .	1376
(PAOLO GUARDA)	

<b>Art. 111</b>	<i>Regole deontologiche per trattamenti nell'ambito del rapporto di lavoro.</i> . . . . .	1381
	(ILARIO ALVINO)	
<b>Art. 111-bis</b>	<i>Informazioni in caso di ricezione di curriculum</i> . . . . .	1384
	(ILARIO ALVINO)	
<b>Art. 112</b>	[ <i>Finalità di rilevante interesse pubblico</i> ] . . . . .	1386
<b>Art. 113</b>	<i>Raccolta di dati e pertinenza</i> . . . . .	1386
	(ILARIO ALVINO)	
<b>Art. 114</b>	<i>Garanzie in materia di controllo a distanza</i>	
<b>Art. 115</b>	<i>Telelavoro, lavoro agile e lavoro domestico</i> . . . . .	1393
	(ARTURO MARESCA)	
<b>Art. 116</b>	<i>Conoscibilità di dati su mandato dell'interessato</i> . . . . .	1410
	(ILARIO ALVINO)	
<b>Artt. 117-119</b>	[ <i>Abrogati</i> ] . . . . .	1412
<b>Art. 120</b>	<i>Sinistri</i> . . . . .	1412
	(AMARILLIDE GENOVESE)	
<b>Art. 121</b>	<i>Servizi interessati e definizioni</i> . . . . .	1420
	(ELENA PODDIGHE)	
<b>Art. 122</b>	<i>Informazioni raccolte nei riguardi del contraente o dell'utente</i> . . . . .	1431
	(ELENA PODDIGHE)	
<b>Art. 123</b>	<i>Dati relativi al traffico</i>	
<b>Art. 124</b>	<i>Fatturazione dettagliata</i>	
<b>Art. 125</b>	<i>Identificazione della linea</i>	
<b>Art. 126</b>	<i>Dati relativi all'ubicazione</i>	
<b>Art. 127</b>	<i>Chiamate di disturbo e di emergenza</i>	
<b>Art. 128</b>	<i>Trasferimento automatico della chiamata</i> . . . . .	1444
	(ELENA PODDIGHE)	
<b>Art. 129</b>	<i>Elenchi dei contraenti</i>	
<b>Art. 130</b>	<i>Comunicazioni indesiderate</i> . . . . .	1472
	(ELENA PODDIGHE)	
<b>Art. 131</b>	<i>Informazioni a contraenti e utenti</i>	
<b>Art. 132</b>	<i>Conservazione di dati di traffico per altre finalità</i> . . . . .	1487
	(ELENA PODDIGHE)	
<b>Art. 132-bis</b>	<i>Procedure istituite dai fornitori</i> . . . . .	1501
	(EDOARDO RUZZI)	
<b>Art. 132-ter</b>	<i>Sicurezza del trattamento</i> . . . . .	1505
	(EDOARDO RUZZI)	
<b>Art. 132-quater</b>	<i>Informazioni sui rischi</i> . . . . .	1514
	(EDOARDO RUZZI)	
<b>Art. 133</b>	[ <i>Codice di deontologia e di buona condotta</i> ] . . . . .	1518
<b>Art. 134</b>	[ <i>Codice di deontologia e di buona condotta</i> ] . . . . .	1518
<b>Art. 135</b>	[ <i>Profili generali</i> ] . . . . .	1519



<b>Art. 136</b>	<i>Finalità giornalistiche e altre manifestazioni del pensiero.</i>	
<b>Art. 137</b>	<i>Disposizioni applicabili.</i>	
<b>Art. 138</b>	<i>Segreto professionale.</i> . . . . .	1520
	(CARLO MELZI D'ERIL e GIULIO ENEA VICEVANI)	
<b>Art. 139</b>	<i>Regole deontologiche relative ad attività giornalistiche.</i> . . . . .	1539
	(NICOLA CANZIAN e SILVIA VIMERCATI)	
<b>Art. 140</b>	[ <i>Codice di deontologia e di buona condotta</i> ] . . . . .	1546
<b>Art. 140-bis</b>	<i>Forme alternative di tutela.</i> . . . . .	1547
	(PAOLA CHIARA RUGGIERI)	
<b>Art. 141</b>	<i>Reclamo al Garante.</i> . . . . .	1555
	(GIOVANNI GUERRA)	
<b>Art. 142</b>	<i>Proposizione del reclamo.</i> . . . . .	1559
	(GIOVANNI GUERRA)	
<b>Art. 143</b>	<i>Decisione del reclamo.</i> . . . . .	1563
	(GIOVANNI GUERRA)	
<b>Art. 144</b>	<i>Segnalazioni.</i> . . . . .	1567
	(GIOVANNI GUERRA)	
<b>Artt. 145-151</b>	[ <i>Abrogati</i> ] . . . . .	1569
<b>Art. 152</b>	<i>Autorità giudiziaria ordinaria.</i> . . . . .	1569
	(Rinvio agli artt. 78 e 79 GDPR)	
<b>Art. 153</b>	<i>Garante per la protezione dei dati personali.</i> . . . . .	1570
	(MARINA CAPORALE)	
<b>Art. 154</b>	<i>Compiti.</i> . . . . .	1582
	(GIOVANNI GUERRA)	
<b>Art. 154-bis</b>	<i>Poteri.</i> . . . . .	1592
	(PAOLA CHIARA RUGGIERI)	
<b>Art. 154-ter</b>	<i>Potere di agire e rappresentanza in giudizio.</i> . . . . .	1600
	(PAOLA CHIARA RUGGIERI)	
<b>Art. 155</b>	<i>Ufficio del Garante</i>	
<b>Art. 156</b>	<i>Ruolo organico e personale.</i> . . . . .	1608 <sup>***</sup>
	(FRANCESCO CARDARELLI)	
<b>Art. 157</b>	<i>Richiesta di informazioni e di esibizione di documenti.</i> . . . . .	1627
	(GIOVANNI GUERRA)	
<b>Art. 158</b>	<i>Accertamenti.</i> . . . . .	1633
	(GIOVANNI GUERRA)	
<b>Art. 159</b>	<i>Modalità.</i> . . . . .	1639
	(GIOVANNI GUERRA)	
<b>Art. 160</b>	<i>Particolari accertamenti.</i> . . . . .	1645
	(GIOVANNI GUERRA)	

INDICE SISTEMATICO

<b>Art. 160-bis</b> <i>Validità, efficacia e utilizzabilità nel procedimento giudiziario di atti, documenti e provvedimenti basati sul trattamento di dati personali non conforme a disposizioni di legge o di regolamento</i> . . . . .	1649
(GIOVANNI GUERRA)	
<b>Artt. 161-165</b> [Abrogati] . . . . .	1653
<b>Art. 166</b> <i>Criteri di applicazione delle sanzioni amministrative pecuniarie e procedimento per l'adozione dei provvedimenti correttivi e sanzionatori</i> . . . . .	1653
(GIOVANNI GUERRA)	
<b>Art. 167</b> <i>Trattamento illecito di dati</i>	
<b>Art. 167-bis</b> <i>Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala</i>	
<b>Art. 167-ter</b> <i>Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala</i>	
<b>Art. 168</b> <i>Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante.</i>	
<b>Art. 169</b> [Misure di sicurezza]	
<b>Art. 170</b> <i>Inosservanza di provvedimenti del Garante</i>	
<b>Art. 171</b> <i>Violazioni delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori</i>	
<b>Art. 172</b> <i>Pene accessorie.</i> . . . . .	1669
(VITTORIO MANES e FRANCESCO MAZZACUVA)	
<b>Artt. 173-174</b> [Abrogati] . . . . .	1684
<b>Art. 175</b> <i>Forze di polizia.</i> . . . . .	1684
(FEDERICA RESTA)	
<b>Artt. 176-179</b> [Abrogati] . . . . .	1688
<b>Artt. 180-182</b> [Abrogati] . . . . .	1689
<b>Art. 183</b> <i>Norme abrogate.</i> . . . . .	1689
(MARIA CHIARA MENEGHETTI)	
<b>Artt. 184-185</b> [Abrogati] . . . . .	1698
<b>Art. 186</b> <i>Entrata in vigore.</i> . . . . .	1698
(MARIA CHIARA MENEGHETTI)	
 <b>D.lgs. 10 agosto 2018, n. 101. — Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)</b>	
<b>Art. 17</b> <i>Modifiche al decreto legislativo 1° settembre 2011, n. 150.</i> . . . . .	1705
(VALERIO LUBELLO)	
<b>Art. 18</b> <i>Definizione agevolata delle violazioni in materia di protezione dei dati personali.</i> . . . . .	1712
(VALERIO LUBELLO)	
<b>Art. 19</b> <i>Trattazione di affari pregressi.</i> . . . . .	1716
(VALERIO LUBELLO)	

<b>Art. 20</b>	<i>Codici di deontologia e di buona condotta vigenti alla data di entrata in vigore del presente decreto</i> . . . . .	1719
	(ROBERTO D'ORAZIO)	
<b>Art. 21</b>	<i>Autorizzazioni generali del Garante per la protezione dei dati personali.</i> . . . . .	1724
	(GIOVANNI DE GREGORIO)	
<b>Art. 22</b>	<i>Altre disposizioni transitorie e finali.</i> . . . . .	1730
	(FEDERICO RUGGERI)	
<b>Art. 23</b>	<i>Disposizioni di coordinamento.</i> . . . . .	1741
	(FEDERICO RUGGERI)	
<b>Art. 24</b>	<i>Applicabilità delle sanzioni amministrative alle violazioni anteriormente commesse.</i>	
<b>Art. 25</b>	<i>Trasmissione degli atti all'autorità amministrativa.</i> . . . . .	1748
	(FRANCESCO MAZZACUVA)	
<b>Art. 26</b>	<i>Disposizioni finanziarie.</i> . . . . .	1753
	(VALERIO LUBELLO)	
<b>Art. 27</b>	<i>Abrogazioni.</i> . . . . .	1754
	(EDOARDO RUZZI)	
	<i>Tabella delle corrispondenze</i> . . . . .	1761
	<i>Indice analitico</i> . . . . .	1765

€ 195,00  
024206123

ISBN 978-88-28-82256-1



9 788828 822561