GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Parere su uno schema di decreto del Presidente del Consiglio dei ministri concernente la disciplina di attuazione della disposizione di cui all’articolo 2 della legge 19 giugno 2019, n. 56, recante “Interventi per la concretezza delle azioni delle pubbliche amministrazioni e la prevenzione dell'assenteismo” - 19 settembre 2019 [9147290]

[doc. web n. 9147290]

Parere su uno schema di decreto del Presidente del Consiglio dei ministri concernente la disciplina di attuazione della disposizione di cui all’articolo 2 della legge 19 giugno 2019, n. 56, recante “Interventi per la concretezza delle azioni delle pubbliche amministrazioni e la prevenzione dell'assenteismo” - 19 settembre 2019

Registro dei provvedimenti
n. 167 del 19 settembre 2019

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del dott. Antonello Soro, presidente, della dott.ssa Augusta Iannini, vice presidente, della prof.ssa Licia Califano e della dott.ssa Giovanna Bianchi Clerici, componenti e del dott. Giuseppe Busia, segretario generale;

Vista la richiesta di parere della Presidenza del Consiglio dei ministri – Dipartimento per gli affari giuridici e legislativi;

Visto l’articolo 36, par. 4, 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, di seguito Regolamento);

Visto il Codice in materia di protezione dei dati personali, recante disposizioni per l’adeguamento dell’ordinamento nazionale al 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 (decreto legislativo n. 196 del 2003, come modificato dal decreto legislativo 10 agosto 2018, n. 101, di seguito Codice);

Visto l’articolo 2 della legge 19 giugno 2019, n. 56;

Vista la documentazione in atti;

Viste le osservazioni dell’Ufficio ai sensi dell’art. 15 del regolamento del Garante n. 1/2000;

Relatore il dott. Antonello Soro;

PREMESSO

1. La Presidenza del Consiglio dei ministri – Ufficio legislativo del Ministro per la pubblica amministrazione ha richiesto il parere dell’Autorità su uno schema di decreto del Presidente del Consiglio dei ministri concernente la disciplina di attuazione della disposizione di cui all’articolo 2 della legge 19 giugno 2019, n. 56, recante “Interventi per la concretezza delle azioni delle pubbliche

amministrazioni e la prevenzione dell'assenteismo".

Il menzionato articolo 2 stabilisce che "Ai fini della verifica dell'osservanza dell'orario di lavoro, le amministrazioni pubbliche di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, con esclusione dei dipendenti di cui all'articolo 3 del medesimo decreto e fuori dei casi di cui all'articolo 18 della legge 22 maggio 2017, n. 81, introducono (…) sistemi di verifica biometrica dell'identità e di videosorveglianza degli accessi, in sostituzione dei diversi sistemi di rilevazione automatica, attualmente in uso, nel rispetto dei principi di proporzionalità, non eccedenza e gradualità sanciti dall'articolo 5, paragrafo 1, lettera c), del regolamento (UE) 2016/679 (…) e del principio di proporzionalità previsto dall'articolo 52 della Carta dei diritti fondamentali dell'Unione europea. ".

La medesima disposizione rimette la disciplina attuativa ad un decreto del Presidente del Consiglio dei ministri, adottato ai sensi dell'articolo 17, comma 3, della legge 23 agosto 1988, n. 400, su "proposta del Ministro per la pubblica amministrazione, previa intesa in sede di Conferenza unificata […] e previo parere del Garante per la protezione dei dati personali…", nel rispetto dell'articolo 9 del Regolamento (UE) 2016/679 e delle misure di garanzia definite dal Garante ai sensi dell'articolo 2-septies Codice.

Sullo schema di disegno di legge, poi approvato dal Parlamento, il Garante, nell'esercizio dei propri poteri consultivi sugli atti normativi, ha reso parere nell'ottobre scorso (art. 36, par. 4, Reg.; parere 11 ottobre 2018, n. 464, doc. web n. 9051774).

Successivamente, nel corso dei lavori parlamentari per l'approvazione del disegno di legge il Garante ha poi tenuto una prima audizione presso la Commissione Lavoro pubblico e privato, previdenza sociale del Senato (il 27 novembre 2018, doc. web n. 9064421) ed una seconda presso le Commissioni riunite Affari Costituzionali e Lavoro della Camera dei Deputati (il 6 febbraio 2019, doc. web n. 9080870).

RILEVATO

2. Lo schema di regolamento delinea la disciplina di attuazione della disposizione di rango primario, individuando i criteri, le modalità e i termini ai quali le amministrazioni dovranno attenersi per la realizzazione dei sistemi di rilevamento biometrico e di videosorveglianza necessari per la realizzazione delle misure di contrasto del fenomeno dell'assenteismo sul posto di lavoro nelle pubbliche amministrazioni.

In particolare, l'articolo 1, come si legge nella relazione illustrativa dello schema di regolamento reca le "definizioni", necessarie ad una corretta interpretazione del provvedimento, quali: "verifica biometrica" (processo attraverso il quale il soggetto dichiara la sua identità e il sistema di verifica effettua un confronto in tempo reale fra le informazioni biometriche rilevate e quelle memorizzate su dispositivo sicuro e corrispondenti all'identità dichiarata); "informazioni biometriche" (codice alfanumerico generato da un algoritmo a partire dalle caratteristiche biometriche del soggetto); "registrazione" (processo di acquisizione e calcolo delle informazioni biometriche del soggetto e registrazione ai fini del trasferimento su un dispositivo sicuro); "dispositivi sicuri" (mezzi sui quali il soggetto può conservare un controllo esclusivo e sui quali sono memorizzate le informazioni biometriche corrispondenti alla sua identità); "dispositivo di acquisizione del dato biometrico" (mezzo mediante il quale si acquisiscono le caratteristiche biometriche dell'utente tramite apposito hardware e software); "template biometrico" (l'insieme di valori numerici estratti da un campione biometrico, che ne descrivono caratteristiche utili ai fini della verifica dell'identità del titolare).

L'articolo 2 definisce l'oggetto e l'ambito di applicazione del provvedimento, espressamente rivolto alle amministrazioni pubbliche di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165 e al relativo personale con rapporto di lavoro subordinato. È escluso dall'ambito di applicazione del regolamento il personale in regime di diritto pubblico di cui all'articolo 3, del decreto legislativo n. 165 del 2001 (ad es. i magistrati ordinari, amministrativi e contabili, gli avvocati e procuratori dello Stato, il personale militare e delle Forze di polizia, il personale della carriera diplomatica e della carriera prefettizia).

L'articolo 3 disciplina le modalità di "acquisizione delle informazioni biometriche", prevedendo che detta attività si svolga, previa informazione e in presenza del soggetto interessato, mediante sistemi in grado di acquisire le caratteristiche biometriche dello stesso, calcolando in tempo reale le corrispondenti informazioni biometriche e memorizzando le medesime in forma crittografata sul dispositivo sicuro. È previsto che i sistemi di acquisizione siano protetti contro i rischi di accesso abusivo di cui all'art. 615-ter del codice penale.

L'articolo 4 individua le "caratteristiche dei sistemi di verifica biometrica dell'identità", prevedendo che i sistemi siano basati su apparati di rilevazione delle informazioni biometriche installati presso i varchi di accesso alle sedi delle amministrazioni pubbliche e

che questi siano gli unici ad essere abilitati alla lettura delle informazioni biometriche memorizzate sul dispositivo sicuro.

In caso di verifica biometrica positiva, la data e l'ora di attraversamento del varco di accesso al posto di lavoro sono considerati validi ai fini della verifica della presenza e dell'osservanza dell'orario di lavoro da parte del soggetto.

L'articolo 5 disciplina l'attività di videosorveglianza degli accessi, prevedendo che, fermi restando gli obblighi e i divieti previsti dalla disciplina sul lavoro e sulla protezione dei dati personali, gli accessi agli uffici delle pubbliche amministrazioni sono controllati da dispositivi di videosorveglianza installati in prossimità dei rilevatori di presenza in grado di acquisire le immagini relative all'attraversamento del varco ed al verso di attraversamento, in ingresso o in uscita.

La disposizione, inoltre, stabilisce che l'accesso alle immagini registrate debba essere tracciato anche tramite apposite funzionalità che consentano la conservazione delle informazioni sugli accessi per un periodo di tempo non inferiore a sei mesi.

Per l'eventuale trasmissione tramite una rete pubblica di comunicazioni di immagini riprese da apparati di videosorveglianza, è previsto che la stessa sia effettuata attraverso l'utilizzo di tecniche crittografiche che ne garantiscano la riservatezza.

La disposizione, infine, prevede che il personale addetto alla videosorveglianza segnali, con tempestività, ogni eventuale comportamento non coerente con i fini della verifica dell'osservanza dell'orario di lavoro.

L'articolo 6 riguarda i sistemi di verifica biometrica dell'identità e di videosorveglianza degli accessi ai fini della verifica dell'osservanza dell'orario di lavoro prevedendo che tali sistemi debbano consentire di identificare, individuare e rilevare ciò che avviene in prossimità dei varchi di accesso, al fine di consentire di segnalare qualsiasi "evento anomalo" o sospetto, sia del personale dell'amministrazione che di visitatori e di personale non dipendente dell'amministrazione.

Inoltre, si qualifica come "evento anomalo" sia l'attraversamento di un varco di accesso senza che sia avvenuta la rilevazione biometrica, sia la rilevazione biometrica attestante, rispettivamente, l'entrata o l'uscita del soggetto laddove le immagini della videosorveglianza rilevino, rispettivamente, l'uscita o l'entrata del soggetto.

L'articolo 7 disciplina le "modalità di approvvigionamento dei sistemi di verifica biometrica dell'identità e di videosorveglianza degli accessi", stabilendo che gli strumenti necessari allo svolgimento dell'attività di verifica biometrica possano essere acquisiti mediante ricorso agli strumenti di acquisto e di negoziazione messi a disposizione da Consip S.p.A. e dalle centrali di committenza regionali di riferimento, nonché attraverso autonome procedure nel rispetto della normativa vigente, utilizzando di regola i sistemi telematici di negoziazione messi a disposizione dalle stesse amministrazioni.

L'articolo 8 prevede che le pubbliche amministrazioni, che sono tenute a utilizzare i servizi di pagamento degli stipendi messi a disposizione dal Ministero dell'economia e delle finanze, provvedano all'attuazione delle misure del presente regolamento avvalendosi dei servizi di rilevazione delle presenze forniti dal sistema «NoiPA» del Ministero dell'economia e delle finanze, appositamente implementata adeguando i servizi di rilevazione delle presenze attualmente in uso per renderli coerenti con i principi, le finalità e le modalità attuative disciplinate dal presente regolamento.

Le modalità tecnico-organizzative di erogazione degli ulteriori servizi della piattaforma «NoiPA» saranno definite attraverso apposite convenzioni tra le amministrazioni centrali ed il Ministero dell'economia e delle finanze.

RITENUTO

3. La legge n. 56 del 2019 e le criticità rappresentate dal Garante.

Nell'esprimere il richiesto parere, non si può omettere di rilevare come la norma di legge che lo schema di regolamento è tenuto ad attuare presenti profili di dubbia compatibilità con la disciplina europea e nazionale in materia di protezione dei dati personali, come già rilevato dal Garante in sede di parere sullo schema di disegno di legge, nonché di audizione dinanzi alle Commissioni parlamentari competenti.

Sotto un primo profilo, infatti, la previsione dell'obbligatorio impiego contestuale di due sistemi di verifica del rispetto dell'orario di lavoro (raccolta di dati biometrici e videosorveglianza) contrasta con l'esigenza di stretta necessità del trattamento rispetto al fine perseguito; esigenza tanto più rilevante rispetto ai dati biometrici, annoverati nella categoria di dati personali cui la disciplina

europea accorda maggiore tutela.

Se, infatti, presupposto per l'introduzione di un sistema di attestazione della presenza in servizio così invasivo quale quello biometrico è la sua ritenuta efficacia e affidabilità, ne consegue necessariamente l'ultroneità del ricorso contestuale alla videosorveglianza, che nulla potrebbe aggiungere in termini di contrasto di fenomeni elusivi. A ciò si aggiunga che i sistemi di videosorveglianza non sono strumenti idonei, di per sé, ad assolvere alla specifica finalità di rilevazione e di computo dell'orario di lavoro.

Sotto questo profilo, quindi, l'utilizzo contestuale dei due sistemi di attestazione della presenza in servizio appare incompatibile con il canone di proporzionalità di cui all'articolo 52 della Carta dei diritti fondamentali dell'Unione europea e agli articoli 5, paragrafo 1, lettera c) e -relativamente ai dati biometrici - 9, par. 2, lett. b) e g) del Regolamento.

Per altro verso, la norma non sembra conforme a tali principi laddove intenda– come parrebbe dato il tenore letterale – configurare la rilevazione biometrica (unitamente peraltro alle videoriprese) quale obbligatoria in ogni pubblica amministrazione. Infatti, non può ritenersi in alcun modo conforme al canone di proporzionalità- come declinato dalla giurisprudenza europea e interna– l'ipotizzata introduzione sistematica, generalizzata e indifferenziata per tutte le pubbliche amministrazioni di sistemi di rilevazione biometrica delle presenze, in ragione dei vincoli posti dall'ordinamento europeo sul punto, a motivo dell'invasività di tali forme di verifica e delle implicazioni derivanti dalla particolare natura del dato.

Il canone di proporzionalità, infatti, consente il ricorso alle misure più invasive solo a fronte dell'inidoneità allo scopo di sistemi meno limitativi del diritto, dal momento che "deroghe e restrizioni" ai diritti fondamentali devono intervenire "entro i limiti dello stretto necessario" (cfr. Cgue, C-362/14, Maximillian Schrems c. Data Protection Commissioner [GC], 6 ottobre 2015 nonché le sentenze 20 maggio 2003, nelle cause riunite C-465/00, C-138/01 e C-139/01, Österreichischer Rundfunk e altri, e 9 novembre 2010, nelle cause riunite C-92/09 e 93/09, Volker und Markus Schecke e Eifert) . Il test di proporzionalità si articola, dunque, nella duplice valutazione del carattere non sproporzionato degli oneri imposti rispetto ai legittimi fini perseguiti e, quindi, della scelta della misura meno restrittiva dei diritti coinvolti.

Analoga valorizzazione del principio di proporzionalità si riscontra nella recente sentenza n. 20 del 2019 con cui la Corte costituzionale, proprio con riferimento al diritto alla protezione dei dati personali nel bilanciamento, in questo caso, con il principio di trasparenza amministrativa, ha dichiarato incompatibile con i principi di ragionevolezza e proporzionalità gli obblighi di pubblicità reddituale e patrimoniale indifferenziatamente previsti, per tutti i dirigenti pubblici, dalla disciplina vigente.

In tale sede, la Corte ha confermato come "deroghe e limitazioni alla tutela della riservatezza [dei] dati devono operare nei limiti dello stretto necessario, essendo indispensabile identificare le misure che incidano nella minor misura possibile sul diritto fondamentale, pur contribuendo al raggiungimento dei legittimi obiettivi sottesi alla raccolta e al trattamento dei dati".

Pertanto, l'astratta, generalizzata e indifferenziata presunzione (di cui all'art. 2 della legge n. 56 del 2019) di sussistenza, per tutte le amministrazioni pubbliche, di fattori di rischio tali da far ritenere quello biometrico l'unico sistema in grado di assicurare il rispetto dell'orario di lavoro non appare compatibile con il principio di proporzionalità.

Il mero richiamo ai principi di cui all'articolo 5, par. 1, lett. c), del Regolamento, in quanto abbinato alla previsione dell'obbligatorietà della rilevazione biometrica in ogni p.a., unitamente peraltro alla videosorveglianza degli accessi, appare inidonea a escludere il contrasto della disposizione con la disciplina europea.

Né, del resto, tale contrasto verrebbe sanato riferendo il rispetto del canone di proporzionalità alle specifiche modalità attuative di tale obbligo di rilevazione biometrica (modulando diversamente, ad esempio, le tipologie di dati utilizzati o il termine di conservazione), che potrebbe soltanto ridurre l'impatto sul diritto alla protezione dei dati degli interessati, non già eliminare il vizio che connota in radice la norma. L'incompatibilità di tale previsione con i principi di proporzionalità, non eccedenza, minimizzazione risiede infatti nell'an prima che nel quomodo del trattamento: nella sua configurazione come astrattamente obbligatoria a prescindere da qualsiasi esigenza concreta e specifica in tal senso.

Le criticità rilevate a proposito dell'articolo 2 della legge n. 56 del 2019 che - si sottolinea - deve essere oggetto di comunicazione alla Commissione europea ai sensi dell'articolo 88, par. 3, del Regolamento, si estendono quindi, inevitabilmente, anche allo schema di regolamento chiamato ad attuarne il disposto.

4. Lo schema di regolamento.

Ferma restando l'esigenza di modificare la disposizione di cui all'articolo 2 della legge 56 – la cui dubbia legittimità si estende altrimenti, inevitabilmente, alle sue norme attuative – in riscontro alla richiesta di parere di codesta Amministrazione, si indicano, di seguito, alcune misure volte a minimizzare l'impatto dei sistemi di rilevazione previsti sulla protezione dei dati degli interessati, che potranno essere anche tenute in considerazione, nella loro valenza generale, in sede di eventuale stesura del nuovo testo legislativo e, comunque, ai fini della redazione del regolamento di attuazione.

4.1. Il sistema di verifica biometrica dell'identità.

Al sistema di verifica biometrica dell'identità sono dedicati gli articoli 3 e 4 dello schema, mentre all'articolo 1 si rinvengono le pertinenti definizioni.

Innanzitutto, sotto il profilo della terminologia adoperata, è necessario sostituire integralmente la locuzione "informazioni biometriche" e la relativa definizione (art. 1, comma 1, lett. c), dello schema) con quella di "dati biometrici" contenuta nel Regolamento (art. 4, n. 15).

Quanto alla definizione di "template biometrico" (art. 2, comma 1, lett. g)), non appare adeguata la locuzione: "Il template non consente, a partire da esso, la ricostruzione del campione biometrico originale"; oltretutto non si comprende cosa debba intendersi per "campione biometrico originale". Ciò premesso, si suggerisce di allineare le definizioni a quelle di cui al Provvedimento generale del Garante in materia di biometria citato pure nelle premesse del regolamento (Provvedimento generale prescrittivo in materia di biometria del 12 novembre 2014, n. 513, doc. web n. 3556992).

Per quanto riguarda, invece, le modalità di utilizzo del sistema di verifica biometrica, l'articolo 3 deve essere integrato precisando che i dati biometrici di confronto, utilizzati dal personale di controllo dei varchi per effettuare la verifica al momento del passaggio, devono essere memorizzati su un dispositivo sicuro dato nell'esclusiva disponibilità dell'interessato, che deve essere consegnato a quest'ultimo immediatamente al termine della fase di registrazione, contestualmente alla cancellazione di ogni altra copia dei dati.

All'articolo 4, sarebbe opportuno precisare che i dati biometrici forniti dagli interessati al momento del passaggio presso i varchi di accesso non possono essere memorizzati, se non per il tempo strettamente necessario alla verifica, avvenuta la quale devono essere immediatamente cancellati.

E' necessario poi richiamare le misure di sicurezza individuate nei paragrafi 4.2 e 4.3 del citato provvedimento generale del Garante in materia di biometria del 2014.

Lo schema non contiene, peraltro, alcuna indicazione in ordine alle specifiche caratteristiche del trattamento che si intende consentire, anche con riguardo alla tecnologia ritenuta appropriata in ragione dell'obiettivo perseguito, come invece suggerito nel parere del 2018 (cfr. par. 4). A tal fine, occorre quindi procedere a tale specificazione, prediligendo tra le principali caratteristiche biometriche quelle che abbiano proprietà meno "invasive" e in cui il rilevamento dei dati biometrici debba avvenire con la necessaria collaborazione dell'interessato.

Sarebbe opportuno, inoltre, inserire nello schema di regolamento la previsione di un sistema alternativo per i casi in cui gli interessati non possano, anche in ragione di proprie caratteristiche fisiche, servirsi del sistema di riconoscimento biometrico, dandone conto nell'informativa da rendere agli interessati.

Più in generale, infine, è opportuno sottolineare l'obbligo di fornire un'idonea informativa agli interessati ai sensi dell'art. 13 del Regolamento enunciando le cautele adottate (es. l'assenza di centralizzazione dei dati) e i tempi di conservazione dei dati.

4.2. Impiego di sistemi di videosorveglianza.

Preliminarmente si ribadisce che continuano a permanere profili di forte criticità con riferimento all'impiego simultaneo dei sistemi di rilevazione biometrica e di videosorveglianza.

Quanto all'utilizzo dei sistemi di videosorveglianza, per una maggiore aderenza al dettato normativo di rango primario, all'articolo 5, comma 1, dello schema è opportuno sostituire le parole da "installati" sino alla fine del comma con le seguenti: "installati in

prossimità degli accessi e degli ingressi".

Ciò, anche alla luce del tenore dell'articolo 6 dello schema in esame, che fa riferimento alla necessità di rilevare "qualsiasi evento anomalo o sospetto sia del personale dell'amministrazione" che di altri soggetti (cui non dovrebbe trovare applicazione la disciplina in esame), ossia "visitatori" e "personale non dipendente dell'amministrazione" (es. personale di ditte esterne, o con diversa tipologia contrattuale, consulenti, tirocinanti che non abbiano comunque un rapporto di lavoro subordinato), da cui sembra emergere come, nell'intento regolatorio, l'introduzione dei sistemi di videosorveglianza assolva (più che a finalità di rilevazione dell'orario di lavoro, rispetto alla quale, peraltro, risulta di per sé inidonea) alla più ampia finalità di sicurezza degli accessi, che ben potrebbe essere efficacemente perseguita attraverso l'installazione di telecamere in prossimità degli ingressi o di altri punti di accesso all'edificio, senza essere orientate sul sistema di rilevazione delle presenze.

Si richiama l'attenzione inoltre sul rispetto in concreto della disciplina in materia di controlli a distanza dell'attività lavorativa dei dipendenti, al di là del generico richiamo contenuto nel comma 1 dell'articolo (art. 4, l. 20.5.1970, n. 300, come modificata dal d.lg. 14 settembre 2015, n. 151, cui rinvia l'art. 114 del Codice, la cui formulazione è stata confermata in sede di adeguamento della disciplina nazionale alle disposizioni del Regolamento: d.lg. n. 101/2018), tenuto conto del disposto dell'articolo 88, par. 2, del Regolamento che fa salve le norme nazionali in materia di diritto del lavoro purché contengano "misure appropriate e specifiche" per la salvaguardia della "dignità umana, degli interessi legittimi e dei diritti fondamentali degli interessati", attesa la maggiore intrusività e il minor grado di consapevolezza e aspettativa di essere monitorati nei luoghi di lavoro.

Sotto questo profilo, sarebbe opportuno precisare nello schema di regolamento che le videocamere non saranno orientate su eventuale personale di vigilanza (cfr. art. 5, comma 6).

Inoltre, devono essere individuati i tempi di conservazione delle immagini riprese da tali apparati, tenuto conto di quanto stabilito dal Provvedimento generale in materia di videosorveglianza adottato dal Garante l'8 aprile 2010, in cui si stabilisce che "la conservazione deve essere limitata a poche ore o, al massimo, alle ventiquattro ore successive alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici o esercizi, nonché nel caso in cui si deve aderire ad una specifica richiesta investigativa dell´autorità giudiziaria o di polizia giudiziaria" e di quanto indicato al paragrafo 119 delle recenti Guidelines 3/2019 on processing of personal data through video devices, adottate dal European Data Protection Board il 10 luglio 2019 e ora sottoposte a consultazione pubblica.

Relativamente alla conservazione delle immagini, devono poi essere dettagliate le misure di sicurezza che le amministrazioni dovranno adottare per prevenire i rischi di accessi non autorizzati alle immagini stesse.

Deve essere altresì specificata la modalità con cui il sistema di videosorveglianza sarà in grado di effettuare i controlli indicati nell'articolo 6 dello schema di regolamento, con riguardo alla capacità di identificare, individuare e rilevare ciò che avviene in prossimità dei varchi e di segnalare qualsiasi evento anomalo o sospetto. In particolare, laddove tali controlli dovessero avvenire in via automatizzata e non tramite l'esclusivo riscontro effettuato in tempo reale dal personale addetto alla videosorveglianza, si sarebbe in presenza di sistemi di videosorveglianza c.d. "intelligenti", che non si limitano a riprendere e registrare le immagini, ma sono in grado di rilevare automaticamente comportamenti o eventi anomali, segnalarli, ed eventualmente registrarli.

Il combinato disposto degli articoli 5, comma 5, e 6, comma 2 sembra presupporre l'adozione di sistemi integrati di rilevazione delle immagini e di dati biometrici (es. riconoscimento facciale) o che, dialogando con i sistemi di rilevazione biometrica per la rilevazione delle presenze, consentano di segnalare, in automatico, i comportamenti e le anomalie in prossimità degli stessi. Sul punto si rileva, in primo luogo, la mancanza di uno specifico riferimento nella legge (che si limita a menzionare generici sistemi di videosorveglianza) e la particolare invasività della tecnologia in questione.

4.3. Modalità di approvvigionamento dei sistemi e rispetto dei principi di privacy by design e privacy by default.

L'articolo 7 dello schema di d.P.C.M. prevede che le acquisizioni strumentali all'introduzione dei sistemi di verifica biometrica e di videosorveglianza degli accessi avvengano facendo ricorso agli strumenti di acquisto e di negoziazione messi a disposizione da Consip S.P.A.

A tal proposito è necessario che nella selezione dei prodotti, servizi e applicazioni acquistabili attraverso i sistemi telematici di negoziazione di Consip, ovvero nelle procedure ad evidenza pubblica, si tenga conto delle specifiche caratteristiche, anche tecniche degli stessi, prediligendo quelli che, sia nella fase di progettazione che di sviluppo successivo, abbiano proprietà tali da

consentire ai titolari e ai responsabili del trattamento di adempiere agli obblighi di protezione dei dati in conformità ai principi di privacy by design e by default (cfr. considerando 78 e art. 25 Reg.).

4.4. I soggetti.

All'articolo 8, sarebbe opportuno chiarire quali sono i compiti e i ruoli del titolare e del responsabile ai fini della protezione dei dati svolti dai soggetti coinvolti; se dubbi non sussistono infatti sulla titolarità autonoma della singola amministrazione-datore di lavoro, occorre chiarire il ruolo di altri soggetti istituzionali coinvolti, in particolare il Ministero dell'economia e delle finanze, attraverso il sistema informatico "NoiPA", disciplinando i flussi informativi tra le amministrazioni coinvolte.

Con riguardo poi alla Convenzione che il Ministero dell'economia e delle finanze deve stipulare con le amministrazioni che si avvalgono dei servizi di rilevazione delle presenze forniti da "NoiPA" per definire le modalità tecnico-organizzative di erogazione dei servizi – si suggerisce di prevedere l'adozione di uno schema tipo di convenzione, da adottare sentito il Garante.

4.5. Valutazione di impatto sulla protezione dei dati.

La disciplina in esame prevede l'impiego di una tecnologia di trattamento innovativa per il trattamento di dati particolarmente delicati, quelli biometrici, relativi peraltro ad interessati "vulnerabili", quali sono i lavoratori dipendenti in ragione dello squilibrio esistente tra le parti del rapporto. Tenuto conto delle indicazioni fornite sul punto dal Gruppo di lavoro "Articolo 29" e dallo stesso Garante circa il "rischio elevato" che presentano tali trattamenti, si propone di inserire una specifica disposizione nel regolamento che preveda che la singola amministrazione, in qualità di datore di lavoro e titolare del trattamento, prima dell'attivazione del sistema prescelto effettui una valutazione di impatto ai sensi dell'articolo 35 del Regolamento. La valutazione potrà essere effettuata anche da parte di più titolari del trattamento in considerazione delle caratteristiche analoghe delle relative amministrazioni (ad esempio, per il comparto ministeri) - eventualmente secondo uno schema reso disponibile nella convenzione-tipo cui si accennava sopra - e, in ragione dell'interesse pubblico sotteso a tali trattamenti, dovrà essere sottoposta, ai sensi dell'articolo 2-quinquiesdecies del Codice, al Garante, che potrà provvedere anche con provvedimento di carattere generale.

La disposizione potrebbe avere la seguente formulazione:

"Nel rispetto del principio di responsabilizzazione, il titolare del trattamento, previa valutazione di impatto, da sottoporre al Garante ai sensi dell'art. 2-quinquiesdecies del decreto legislativo 30 giugno 2003, n. 196, individua: le categorie di interessati, in ragione delle mansioni svolte, circoscrivendo il numero di soggetti da sottoporre ai controlli; gli ulteriori presupposti per l'adozione dei sistemi in questione, alla luce delle condizioni più specifiche, anche ambientali, delle amministrazioni di riferimento; le caratteristiche tecniche dei sistemi al fine di garantire la selettività degli accessi ed elevati livelli di sicurezza."

TUTTO CIÒ PREMESSO IL GARANTE

esaminato lo schema di decreto del Presidente del Consiglio dei ministri concernente la disciplina di attuazione della disposizione di cui all'articolo 2, della legge 19 giugno 2019, n. 56, recante "Interventi per la concretezza delle azioni delle pubbliche amministrazioni e la prevenzione dell'assenteismo", ai sensi degli articoli 36, par. 4 e 57, par. 1, lett. c), del Regolamento esprime parere nei termini di cui in motivazione, con le osservazioni di cui ai punti da 4.1. a 4.5.

Roma, 19 settembre 2019

IL PRESIDENTE
Soro

IL RELATORE
Soro

IL SEGRETARIO GENERALE
Busia