svolgimento di un'attività formativa indirizzata al personale della sede che ha fatto uso del sistema di gestione documentale, illustrandone compiutamente le funzionalità e le implicazioni in materia di protezione dei dati.

13.2. DATI BIOMETRICI E RAPPORTO DI LAVORO

Con riferimento al trattamento di dati biometrici per la rilevazione delle presenze dei lavoratori il Garante ha ribadito il proprio consolidato orientamento che reputa, di regola, eccedente l'utilizzo di informazioni biometriche per finalità di ordinaria gestione del rapporto di lavoro e, segnatamente, per la commisurazione dell'orario di servizio prestato (cfr. punto 4. provv. 23 novembre 2006, linee-guida per il trattamento di dati dei dipendenti privati [doc. web n. 1364099] e punto 7. provv. 14 giugno 2007, linee-guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico [doc. web n. 1417809]).

Tale orientamento -condiviso da una recente giurisprudenza di merito (Trib. Prato, 19 settembre 2011) e coerente con quanto affermato nel Parere n. 3/2012 sugli sviluppi nelle tecnologie biometriche, adottato in data 27 aprile 2012, dal Gruppo Art. 29 secondo cui "*il datore di lavoro è sempre tenuto a cercare i mezzi meno invasivi scegliendo, se possibile, un procedimento non biometrico*"- si affianca a quello, esso pure consolidato, secondo cui è invece di regola lecito l'utilizzo di tali dati per presidiare l'accesso ad "aree sensibili", anche in considerazione della natura delle attività ivi svolte.

In termini generali, si segnala, altresì, che è risultato frequente l'inadempimento dell'obbligo di notificazione al Garante dei trattamenti effettuati con l'impiego di dispositivi biometrici (cfr. artt. 37 e 163 del Codice).

Venendo alla casistica, in sede di verifica preliminare (*ex* art. 17 del Codice), un comune ha sottoposto al Garante l'installazione di un sistema di rilevazione biometrica basato sulla lettura delle impronte digitali per finalità di rilevazione delle presenze dei dipendenti, volto ad impedire il reiterarsi di fenomeni di uso improprio del *badge* individuale, oggetto di un'indagine dell'autorità giudiziaria. Il Garante ha ritenuto il trattamento non conforme ai princìpi di necessità, pertinenza e non eccedenza (in relazione

agli artt. 3, 11, comma 1, lett. *d*), del Codice), posto che l'ente locale non aveva dato prova dell'insufficienza delle ordinarie modalità di controllo della presenza dei lavoratori -con riferimento sia a sistemi fisici sia a misure tecnico-organizzative di agevole implementazione- in alternativa ai più invasivi sistemi biometrici, l'utilizzo dei quali potrebbe peraltro rivelarsi, in sé, di scarsa utilità nel contrasto dell'assenteismo ove non accompagnata da un'efficace opera di controllo e verifica da parte del datore di lavoro (provv. 31 gennaio 2013 [doc. web n. 2304669]).

In un altro caso il Garante ha accertato che presso un cantiere edile per la ristrutturazione di un immobile, l'accesso delle maestranze ivi impiegate era consentito -unitamente ad altre modalità di accertamento dell'identità dei lavoratori- previa identificazione biometrica effettuata da apposito sistema basato sulla rilevazione della geometria della mano e successiva estrazione del relativo *template*, poi conservato in un unico *database*. Considerata la mancanza di specifici elementi in relazione alla concreta attività svolta dai titolari del trattamento ed alla luce dell'esistenza di concorrenti procedure di identificazione delle maestranze, il Garante non ha ritenuto lecito il sistema biometrico utilizzato (provv. 13 settembre 2012 [doc. web n. 1927456]).

13.3. TRATTAMENTO DI DATI IDONEI A RIVELARE LE OPINIONI SINDACALI

Tra le decisioni relative all'utilizzo di dati personali nell'ambito della gestione del rapporto di lavoro, merita di essere menzionato il provvedimento che ha ritenuto illecito il trattamento effettuato dalla direzione di una casa circondariale di dati sensibili ai sensi dell'art. 4, comma 1, lett. *d*), del Codice, segnatamente dei nominativi del personale di polizia penitenziaria che aveva preso parte ad una manifestazione sindacale (provv. 29 novembre 2012 [doc. web n. 2192643]).

Nella vicenda in esame, il trattamento dei dati sensibili nell'ambito della gestione del rapporto di lavoro, pur se (in astratto) consentito ai fini dell'instaurazione di un eventuale procedimento disciplinare a carico di alcuno dei partecipanti (artt. 20, comma 1, 112, comma 2, lett. *g*), del Codice nonché decreto del Ministro della giustizia 12 dicembre 2006 n. 306, "Regolamento sulla disciplina del trattamento dei dati sensibili e giudiziari da parte del

Ministero della giustizia"), non è risultato lecito (ai sensi degli artt. 11, comma 1, lett. *a)* e 20, comma 1, del Codice) non essendosi rinvenuti i presupposti per disporre alcun procedimento disciplinare a carico dei partecipanti alla manifestazione, né potendo la mera indizione e partecipazione ad una manifestazione sindacale configurare di per sé alcun illecito per l'ordinamento, alla luce della fondamentale libertà di riunione riconosciuta dall'art. 17 della Costituzione nonché dall'art. 19, l. n. 395/1990 che, nell'ambito dell'ordinamento del Corpo di polizia penitenziaria, stabilisce le norme di comportamento nel godimento dei diritti politici, civili e sindacali.

Con il medesimo provvedimento è stato vietato alla direzione della casa circondariale di trattare ulteriormente i dati relativi ai nominativi dei partecipanti alla manifestazione, con loro conservazione per esigenze di tutela dei diritti in sede giudiziaria, ed è altresì stato prescritto di portare a conoscenza dei soggetti cui eventualmente i dati riferiti agli interessati fossero stati comunicati il contenuto del provvedimento, con particolare riguardo al profilo dell'inutilizzabilità dei dati sensibili dei lavoratori.

13.4. INPS

Nel settore oggetto di competenza dell'Istituto si evidenziano essenzialmente casi riguardanti singoli trattamenti.

In dettaglio, il Garante è intervenuto in un caso in cui un cittadino si era visto recapitare, da una filiale dell'Inps, il verbale di accertamento dell'invalidità civile, contenuto in una busta al cui esterno una timbratura rendeva esplicita la sua condizione di disabile.

Al riguardo, l'Autorità ha ribadito che la normativa in materia di protezione dati prevede che i plichi postali non devono recare, sulla parte esterna, segni o indicazioni tali da consentire a soggetti estranei di desumere il contenuto delle comunicazioni ovvero, anche indirettamente, informazioni idonee a rivelare lo stato di salute del destinatario. L'ente previdenziale ha pertanto disposto che le buste utilizzate per l'invio di documentazione sanitaria non rechino indicazioni del genere (nota 18 giugno 2012).

In un'altra occasione, una segnalazione lamentava che una sede dell'Inps aveva inviato una comunicazione circa l'esito della visita per il riconoscimento dell'invalidità civile ad un

soggetto diverso dall'interessato. Il Garante ha invitato l'Istituto ad adottare misure idonee ad evitare il ripetersi della vicenda. Peraltro, in relazione alla comunicazione di dati idonei a rivelare lo stato di salute a persona diversa dell'interessato, l'Ufficio si è riservato, con autonomo procedimento, di verificare i presupposti per contestare la violazione amministrativa (nota 3 settembre 2012).

A seguito di autonomi accertamenti effettuati dall'Ufficio, è stato riscontrato che sul sito istituzionale di una provincia erano consultabili e accessibili a chiunque le graduatorie di disabili, ai fini del collocamento obbligatorio. Il Garante, nel richiamare le indicazioni fornite nelle linee-guida del 2 marzo 2011 [doc. web n. 1793203], ha evidenziato il divieto di diffondere informazioni idonee a rivelare lo stato di salute, che possono essere messe a disposizione *online* solo con modalità che ne impediscano la libera consultabilità in internet. Le amministrazioni possono, pertanto, pubblicare *online* elenchi o documentazione purché accessibili ai soli soggetti richiedenti (e per le sole finalità previste dalla normativa di riferimento) ovvero a coloro che vi abbiano interesse per la tutela di situazioni giuridicamente rilevanti (a tali fini attribuendo per es. idonee credenziali di accesso, quali *username* o *password*, n. di protocollo, ovvero ancora predisponendo, nei siti istituzionali, aree ad accesso selezionato).

A seguito dell'intervento del Garante, la provincia ha rimosso dal sito gli elenchi oggetto di segnalazione, ma l'Ufficio si è riservato di accertare con autonomo procedimento la violazione del divieto di diffondere dati idonei a rivelare lo stato di salute degli interessati (nota 1° ottobre 2012).

Un ufficio periferico dell'Istituto nazionale previdenza sociale ha investito l'Autorità, ai sensi degli artt. 19, comma 2, e 39, comma 2, del Codice, di una richiesta volta a consentire la comunicazione ad un ufficio provinciale del Ministero del lavoro e delle politiche sociali delle informazioni personali contenute nell'estratto contributivo relativo ad alcuni lavoratori (individuati nominativamente) ai sensi dell'art. 3, comma 5, del d.m. 27 ottobre 2004 (disciplina attuativa dell'art. 47, d.l. 30 settembre 2003, n. 269, convertito, con modificazioni, nella l. 24 novembre 2003, n. 326, "Benefici previdenziali per i lavoratori esposti all'amianto"). La comunicazione sarebbe stata effettuata nell'ambito delle finalità istituzionali delle direzioni

provinciali del lavoro, cui il menzionato art. 3 attribuisce un'attività di indagine volta sia a consentire la ricostruzione del *curriculum* professionale dei lavoratori esposti all'amianto in vista del conseguimento dei benefici di legge, sia alla individuazione dell'effettivo datore di lavoro che nel tempo ha provveduto ai versamenti contributivi, nei casi in cui il datore di lavoro, cessato o fallito, sia divenuto irreperibile. Il Garante, riconosciute le finalità istituzionali della comunicazione ha accolto l'istanza, consentendo la comunicazione dei soli dati pertinenti e non eccedenti, funzionali alla redazione del *curriculum* professionale da trasmettere poi successivamente all'Inail, ossia la denominazione del datore di lavoro, il periodo lavorativo e le mansioni, con eventuale indicazione del reparto del lavoratore (provv. 21 marzo 2012 [doc. web n. 1885290]).

13.5. TRATTAMENTO DI DATI PERSONALI E VALUTAZIONI DELLA RICERCA UNIVERSITARIA

Il Presidente dell'Autorità è intervenuto nel dibattito pubblico circa la possibilità di diffondere -con la particolare modalità della pubblicazione *online*- le valutazioni effettuate dall'Anvur (Agenzia nazionale per la valutazione del sistema universitario e della ricerca) sulle attività svolte dalle strutture di ricerca (intervento 3 novembre 2012 [doc. web n. 2086888]). La legittimità del regime di pubblicità dei "prodotti della ricerca" non può che essere valutata alla luce del principio di trasparenza dell'attività amministrativa, preordinato alla realizzazione del buon andamento e dell'imparzialità dell'amministrazione e attuato nei limiti previsti dalla normativa vigente (anche di origine comunitaria) che ne disciplina oggetto, scopi e modalità, in vista del necessario bilanciamento con le esigenze di tutela della riservatezza delle persone. Posto che, in particolare, il Codice consente ai soggetti pubblici di diffondere *online* dati personali solo qualora una norma di legge o di regolamento lo preveda espressamente (art. 19, comma 3) e che l'oggetto della attività valutativa dell'Anvur è, in base alle norme istitutive, la qualità delle strutture universitarie e degli enti di ricerca (non invece dei singoli ricercatori) al fine di predisporre l'allocazione delle risorse finanziarie disponibili, non risulta ancorata ad una idonea base giuridica la pubblicazione in rete dei dati relativi alle valutazioni dei singoli ricercatori. Peraltro, considerato anche che oggetto di valutazione è un numero limitato di pubblicazioni (tre), il giudizio così espresso e reso pubblico potrebbe non

costituire lo strumento più appropriato per rappresentare con modalità trasparenti il merito (o demerito) della produzione scientifica di ciascuno (note 19 settembre 2012).

13.6. PUBBLICAZIONE IN INTERNET DI DATI PERSONALI RELATIVI A LAVORATORI

Numerose sono le segnalazioni ad opera di pubblici dipendenti (o candidati nel settore del pubblico impiego) che lamentano la pubblicazione di dati eccedenti o la persistente pubblicazione in internet, tramite i siti web istituzionali ovvero mediante l'albo pretorio *online*, di vicende personali in difformità dalle previsioni normative.

Esiti di prove di concorso

A tal proposito, può segnalarsi la vicenda di un candidato non ammesso (unitamente ad altri) a sostenere la prova orale di un concorso bandito da un comune nel 2008 e rispetto al quale, a distanza di anni, persistevano sul sito web istituzionale dell'ente reperibili tramite i comuni motori di ricerca, i dati nominativi dei candidati e gli esiti delle prove intermedie sostenute dai partecipanti, compreso il segnalante. Nel premettere che la disciplina di settore dispone che siano pubblicate nell'albo pretorio dell'ente le sole graduatorie definitive dei vincitori di concorso presso gli enti locali territoriali (art. 15, comma 6-*bis*, d.P.R. 9 maggio 1994, n. 487, regolamento recante norme sull'accesso agli impieghi nelle pubbliche amministrazioni e le modalità di svolgimento dei concorsi, dei concorsi unici e delle altre forme di assunzione nei pubblici impieghi), il Garante ha ritenuto illecita la persistente pubblicazione in internet dei dati in parola (artt. 11, comma 1, lett. *a)* e *d)* e 19, comma 3, del Codice; a conferma di altra decisione del Garante cfr., nello stesso senso, Cass. civ., sez. I, 20 luglio 2012, n. 12726). È stato pertanto vietato al comune di diffondere ulteriormente - sia attraverso la pubblicazione nell'albo pretorio *online* che in qualsiasi altra area del sito web istituzionale- i dati personali contenuti nella graduatoria provvisoria del concorso (provv. 6 dicembre 2012 [doc. web n. 2223278]).

In presenza di segnalazioni concernenti l'avvenuta pubblicazione sul sito web del Ministero della giustizia di alcuni dati personali -segnatamente, nomi, cognomi, data di nascita ed esito delle prove scritte riferiti ai candidati del concorso da uditore giudiziario (con la precisazione, per i non ammessi alle prove orali, del giudizio di inidoneità)-, l'Ufficio ha formulato richiesta di informazioni al Ministero evidenziando, tra l'altro, che la disciplina di settore, pur risalente,

si limita a prevedere che "*il risultato completo delle prove scritte sarà reso di pubblica ragione mediante foglio da affiggersi nei locali del Ministero*" (art. 13, ult. comma del r.d. 15 ottobre 1925, n. 1860 - "Modificazioni al regolamento per il concorso di ammissione in magistratura contenuto nel r.d. 19 luglio 1924, n. 1218"). Il Ministero, che aveva prontamente rimosso i dati oggetto di segnalazione dal sito, sulla scorta delle osservazioni del Garante (cfr. linee-guida 2 marzo 2011, cit. punto B.1., nonché provv. 19 aprile 2007 [doc. web n. 1407101], punto 5.), ha quindi provveduto ad introdurre gli accorgimenti tecnici -quali la consultabilità in una sezione del sito web istituzionale degli esiti concorsuali previo inserimento di credenziali individuali, individuate nel codice fiscale e del numero tessera fornita a ciascun candidato in occasione dell'espletamento delle prove- volti ad impedire l'indiscriminata visibilità degli esiti delle prove in internet (nota 23 marzo 2012).

Albo pretorio *online*

Con riferimento alla pubblicazione di atti e documenti nell'albo pretorio *online*, l'Autorità ha definito alcuni procedimenti relativi alla pubblicazione da parte di soggetti pubblici (solitamente enti locali) di atti e documenti riguardanti dipendenti. In alcuni casi la pubblicazione concerneva riferimenti allo stato di salute del lavoratore, dando luogo ad una diffusione di dati vietata ai sensi dell'art. 22, comma 8, del Codice (nonché sanzionata dall'art. 162, comma 2-*bis*, del Codice). Al riguardo, pur potendo le deliberazioni degli organi comunali, consiliari o giuntali, formare oggetto di pubblicazione, l'ente locale titolare aveva l'obbligo di oscurare i riferimenti allo stato di salute dell'interessato (in un caso, peraltro, contenuti in un verbale allegato al provvedimento).

In tali fattispecie è stato ribadito che, alla luce della disciplina in materia di protezione dei dati personali -e conformemente a quanto stabilito nelle linee-guida in materia di trattamento di dati personali contenuti anche in atti e documenti amministrativi, effettuato da soggetti pubblici per finalità di pubblicazione e diffusione sul web del 2 marzo 2011 [doc. web n. 1793203]- nell'adempimento degli obblighi di pubblicazione *online* di atti e provvedimenti amministrativi aventi effetto di pubblicità legale, le amministrazioni possono pubblicare dati personali, anche tratti da atti e documenti amministrativi, qualora "*tale divulgazione, che deve essere sempre sorretta da un'adeguata motivazione, costituisca un'operazione strettamente necessaria al perseguimento delle finalità assegnate all'amministrazione da specifiche leggi o regolamenti*",

salvo in ogni caso il generale e già menzionato divieto di diffusione dei dati relativi allo stato di salute degli interessati (cfr. punto 2.2. linee- guida cit.) (note 12 aprile e 4 luglio 2012).

In altri casi, invece, quando gli atti pubblicati dagli enti locali sono rimasti disponibili sui siti istituzionali oltre il tempo consentito dalla disciplina di settore, con specifico riferimento all'intervallo temporale di diffusione, è stata rilevata l'illiceità del trattamento (artt. 11, comma 1, lett. *a)* e 19, comma 3, del Codice). Infatti, la persistenza delle informazioni personali nell'albo pretorio *online* oltre il termine consentito dalla legge -senza che gli atti o le delibere fossero privati degli elementi identificativi degli interessati- ha reso illecita la diffusione dei dati personali in quanto priva (per il periodo successivo ai quindici giorni previsti dall'art. 124, d.lgs. n. 267/2000 per la pubblicazione nell'albo pretorio) di idonei presupposti normativi (nota 4 luglio 2012).

Come peraltro già chiarito al punto 5.2. delle menzionate linee-guida, trascorsi i periodi di tempo individuati dalla legge per la pubblicazione di atti e provvedimenti amministrativi, i medesimi "*devono essere rimossi dal web o privati degli elementi identificativi degli interessati ovvero, in alternativa, laddove l'ulteriore diffusione dei dati sia volta a soddisfare esigenze di carattere storico-cronologico, gli stessi vanno sottratti all'azione dei comuni motori di ricerca, ad esempio, inserendoli in un'area di archivio consultabile solo a partire dal sito stesso o in un'area ad accesso riservato*" (provv. 23 febbraio 2012 [doc. web n. 1876679]).

Numerose sono state le segnalazioni aventi ad oggetto la pubblicazione sui siti web istituzionali di istituti scolastici, nonché di altri uffici periferici del Ministero dell'istruzione dell'università e della ricerca, di graduatorie di dati personali concernenti il personale docente ovvero il personale amministrativo tecnico ed ausiliario (cd. "ATA") recanti, oltre ai punteggi maturati ed alle generalità degli interessati, anche dati ulteriori quali il numero di codice fiscale, il numero di figli a carico ed i recapiti degli interessati (in particolare nota 8 agosto 2012).

Al riguardo, nelle menzionate linee-guida del 2 marzo 2011 [doc. web n. 1793203] è stato precisato che, in applicazione dei princìpi di liceità, correttezza nonché di pertinenza e non eccedenza (art. 11, comma 1, lett. *a)* e *d)*, del Codice), deve ritenersi eccedente la pubblicazione di dati quali, il recapito di telefonia fissa o mobile, l'indirizzo dell'abitazione o dell'e-mail, i titoli di studio, il codice fiscale.

Nel ribadire che, nello svolgimento di attività istituzionali, la pubblicazione *online* di dati personali deve avvenire, oltre che nel rispetto del Codice, anche osservando la legge e i regolamenti che tale pubblicazione eventualmente prevedono (*ex* artt. 18, 19, comma 3 e 25, del Codice), l'Ufficio ha formulato una richiesta di informazioni al ministero, anche al fine di chiarire il ruolo svolto dagli enti periferici o istituti scolastici nella pubblicazione degli elenchi in esame, i presupposti di legittimità relativi alla diffusione e all'osservanza dei princìpi di necessità (art. 3, del Codice) nonché di pertinenza e non eccedenza della tipologia delle informazioni oggetto di diffusione rispetto alla legittima finalità perseguita (art. 11, comma 1, lett. *d)*, del Codice), oltre che per individuare l'arco temporale durante il quale i menzionati dati personali possono restare visibili in internet.

Merita infine di essere segnalato il provvedimento con il quale il Garante ha vietato la pubblicazione, sul sito di un ateneo, del decreto di annullamento e revoca dell'affidamento di un insegnamento a contratto, risultata non conforme alla disciplina di settore e quindi in violazione del principio di liceità del trattamento di cui all'art. 11, comma 1, lett. *a*) del Codice. Ciò anche in ragione della considerazione che la pubblicazione del provvedimento in parola, contenente le ragioni dell'annullamento del contratto, fosse comunque eccedente rispetto alle finalità perseguite dall'università, in quanto visibile ad una cerchia di soggetti assai più ampia rispetto agli interessati (provv. 12 aprile 2012 [doc. web. 1896533]).

13.7. CONTROLLO A DISTANZA DEI LAVORATORI

La materia del controllo a distanza dei lavoratori (in particolare per il tramite di sistemi di videosorveglianza) e del connesso trattamento di dati personali continua a formare oggetto di numerose segnalazioni indirizzate all'Autorità e di verifiche effettuate *in loco* anche attraverso la Guardia di finanza nonché, nei casi di inosservanza dell'art. 4, l. n. 300/1970, di trasmissione all'Autorità giudiziaria per l'accertamento di violazioni penalmente rilevanti.

In argomento, con riferimento a quanto esposto nella Relazione 2011 (p. 121), è stata respinta dal Tribunale di Roma il 21 gennaio 2013 l'impugnazione avverso il provvedimento del Garante 21 luglio 2011 [doc. web n. 1829641], con il quale sono state ritenute illegittime la conservazione e la categorizzazione, anche su base individuale, dei dati riferiti alla navigazione in internet dei dipendenti di una società di primaria rilevanza.

Videosorveglianza

A seguito degli accertamenti effettuati presso un *call center,* il Garante ha vietato il trattamento dei dati rilevati mediante un sistema di videosorveglianza ivi installato in grado di captare anche le conversazioni dei dipendenti, in violazione dell'art. 4, l. n. 300/1970 (provv. 4 ottobre 2012 [doc. web n. 2066968]). Provvedimenti di analogo contenuto sono stati adottati, in relazione a trattamenti effettuati, in assenza delle garanzie dettate dall'art. 4, l. n. 300/1970, mediante sistemi di videosorveglianza da parte di un hotel (provv. 25 ottobre 2012 [doc. web n. 2212826]) e di un esercizio commerciale (provv. 25 ottobre 2012 [doc. web n. 2212623]).

Il Garante ha dichiarato illecito anche un trattamento effettuato tramite un sistema di videosorveglianza, installato per finalità antitaccheggio presso un negozio, disponendo il blocco del trattamento dei dati. La telecamera riprendeva anche l'area nella quale è posto l'apparecchio per la rilevazione delle presenze dei lavoratori.

In questo caso, è stata ritenuta inidonea l'informativa fornita agli interessati (pur nelle forme semplificate indicate dall'Autorità nel provvedimento generale dell'8 aprile 2010 [doc. web n. 1712680]) ed è stata altresì riscontrata la possibilità (dal punto di vista tecnico) di accedere alle immagini registrate con modalità diverse da quelle stabilite nell'accordo con le rappresentanze sindacali (in violazione dei princìpi di liceità e correttezza nel trattamento). Un ulteriore profilo di illiceità del trattamento è stato ravvisato nella circostanza che il personale incaricato di visionare le immagini per le menzionate finalità antitaccheggio, appartenente a società diversa dal titolare del trattamento, è risultato privo della licenza prefettizia richiesta dalla normativa di settore (art. 134, r.d. 18 giugno 1931, n. 773 (tulps)), con esigenza ribadita sia in relazione al servizio antitaccheggio sia in relazione al servizio di televigilanza (cfr. art. 3, comma 2, lett. *d)*, e lett *f)* d.m. 1° dicembre 2010, n. 269), come peraltro stabilito dal consolidato indirizzo interpretativo della giurisprudenza di legittimità secondo cui "*ogni forma di attività imprenditoriale di vigilanza e custodia di beni per conto terzi esige la licenza del prefetto, indipendentemente dalle modalità operative con le quali viene espletata*" (cfr. Cass. pen., sez. III, 3 dicembre 2010, n. 1821 e ivi ulteriori richiami) (provv. 17 gennaio 2013 [doc. web n. 2291893]).

Ascolto e montaggio delle telefonate dei lavoratori

L'Autorità ha effettuato accertamenti anche in relazione alla registrazione e riascolto delle telefonate effettuate dai lavoratori del *call center* gestito da una cooperativa -la quale eroga

anche il servizio di prenotazione telefonica di prestazioni sanitarie in una regione- nonché al monitoraggio della loro condotta mediante l'analisi del numero e della durata delle conversazioni.

Al riguardo, poiché la registrazione e il riascolto del contenuto delle comunicazioni precedentemente registrate, pur per soddisfare esigenze organizzative o produttive, consentono il controllo a distanza dell'attività dei lavoratori, il Garante ha rilevato che il mancato assolvimento degli adempimenti previsti dall'art. 4, comma 2, l. n. 300/1970 (fatto salvo dall'art. 114 del Codice) riverbera i propri effetti anche sulle operazioni di trattamento dei dati, risultate perciò in violazione dell'art. 11, comma 1, lett. *a)*, del Codice (provv. 1° agosto 2012 [doc. web n. 1923325]; in merito v. provv. 9 febbraio 2011 [doc. web n. 1797032]). Analoga la valutazione sul monitoraggio, in base al loro numero o durata, delle conversazioni di ciascun operatore telefonico -che ha talvolta determinato l'adozione di provvedimenti disciplinari nei confronti dei soci lavoratori- non essendo stati posti in essere dalla società gli adempimenti previsti dall'art. 4, comma 2, l. n. 300/1970.

Geolocalizzazione

Nonostante le prescrizioni impartite in via generale dal Garante con il provvedimento 4 ottobre 2011, n. 370 [doc. web n. 1850581], continuano a formare oggetto di segnalazione trattamenti di dati personali riferiti ai lavoratori effettuati mediante sistemi di geolocalizzazione installati su veicoli aziendali.

In un caso, con riguardo all'impiego di tali sistemi su veicoli assegnati a guardie giurate, il Garante ha ritenuto che il sistema di localizzazione in uso poteva contribuire al conseguimento delle legittime finalità dichiarate dal datore di lavoro, incrementando nel caso di specie anche la sicurezza dei dipendenti; nondimeno, l'impiego di tali strumenti deve avvenire nel rispetto della normativa in materia di protezione dei dati personali. Considerato che il sistema installato consentiva di monitorare a distanza -ancorché non in modo continuo- la posizione del veicolo e, quindi, indirettamente, del lavoratore cui lo stesso era assegnato, il Garante ha rilevato che la società titolare del trattamento non aveva dato attuazione agli adempimenti necessari ai sensi dell'art. 4, comma 2, della l. n. 300/1970, così come richiamato dall'art. 114 del Codice, né reso l'informativa ai dipendenti ai sensi dell'art. 13 del Codice (provv. 1° agosto 2012 [doc. web n. 1923293]).

Nell'ambito di una verifica preliminare presentata ai sensi dell'art. 17 del Codice, il Garante ha invece ritenuto lecito il trattamento di dati personali da parte di una società concessionaria del servizio di trasporto pubblico locale tramite l'installazione di un dispositivo -da apporre sul parabrezza delle vetture e annoverabile tra i cd. "*video event data recorder*" che consente di registrare e -al verificarsi di predeterminate "anomalie"- conservare, immagini relative sia all'interno che all'esterno del veicolo. Le finalità perseguite dalla società (salvaguardia del patrimonio aziendale nonché ricostruzione della dinamica di eventuali sinistri in vista della tutela dei diritti in giudizio) e le concrete modalità di trattamento dei dati (esclusione dell'immagine del conducente dall'angolo di ripresa, offuscamento dei volti di soggetti terzi non coinvolti negli eventi) sono state infatti ritenute conformi ai princìpi di necessità nonché di pertinenza e non eccedenza (artt. 3 e 11, comma 1, lett. *d)*, del Codice). L'Autorità ha ritenuto giustificata la conservazione dei dati registrati per ventiquattro mesi, reputando però eccedente, anche alla luce della sua possibile rilevanza penale (cfr. artt. 617, 617-*bis* e 623-*bis* c.p.) rispetto alle finalità rappresentate, la raccolta e conservazione - prospettata dalla società- di registrazioni della voce delle persone a bordo del veicolo.

I trattamenti effettuati nonché la presenza del dispositivo dovranno comunque essere adeguatamente resi noti, anche attraverso apposita rappresentazione grafica, a tutte le categorie di persone (dipendenti, utenti del servizio ed eventuali terzi) che potrebbero essere interessate dal trattamento (provv. 29 novembre 2012 [doc. web n. 2257616]).

14. LE ATTIVITÀ ECONOMICHE

14.1. SETTORE BANCARIO

A seguito del provvedimento, adottato il 12 maggio 2011 in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie (in G.U. 3 giugno 2011, n. 127 [doc. web n. 1813953]), il Garante ha proseguito nell'attività di collaborazione già avviata con gli operatori del settore.

Con il citato provvedimento -adottato a seguito di segnalazioni e reclami con cui i clienti di alcuni istituti bancari avevano lamentato l'avvenuta effettuazione, presumibilmente da parte di alcuni dipendenti, di accessi indebiti ai loro dati personali (in particolare, informazioni bancarie), poi comunicati a loro insaputa a terzi che li avevano utilizzati per scopi personali (soprattutto nell'ambito di procedimenti di separazione personale e in procedure esecutive)- l'Autorità ha prescritto l'adozione di misure rigorose volte ad impedire illecite operazioni di trattamento ai danni degli interessati. In particolare, è stato stabilito che ogni operazione di accesso ai dati dei clienti, effettuata dagli incaricati del trattamento (sia che comporti movimentazione di denaro, sia di semplice consultazione), dovrà essere tracciata attraverso una serie di elementi, così da consentire alla stessa banca di conoscere chi abbia effettuato il trattamento dei dati e il momento in cui ciò è avvenuto.

A seguito di richieste pervenute da Associazione bancaria italiana (Abi) e Poste Italiane S.p.A., l'Autorità nel 2012 ha intrapreso con tali soggetti un'attività di collaborazione, ancora in corso, volta a fornire chiarimenti in ordine alla corretta applicazione del provvedimento stesso.

Nel corso del 2011 le banche, al fine di contrastare sempre più diffusi fenomeni criminali, hanno rappresentato la necessità di avvalersi di sistemi di videosorveglianza dotati di un *software* "anticamuffamento", in grado di permettere l'individuazione di eventuali rapinatori senza dover ricorrere a strumenti comportanti la rilevazione di impronte digitali. In tale occasione l'Abi, in qualità di rappresentante delle banche, ha chiesto all'Autorità di valutare se le proprie associate fossero effettivamente tenute a presentare una richiesta di verifica preliminare per procedere all'attivazione di tali sistemi.

All'esito dell'attività istruttoria, l'Ufficio ha rappresentato all'Abi (nota 19 dicembre 2011) che il sistema, così come descritto dai titolari del trattamento, sembrerebbe rilevare solo eventuali situazioni di camuffamento, senza procedere ad operazioni di riconoscimento del volto basate sul confronto con immagini contenute in banche dati fotografiche. Il trattamento, pertanto, non è stato ritenuto soggetto a verifica preliminare, sia perché la raccolta dell'immagine dell'interessato non aggiunge nulla di ulteriore rispetto a quanto avviene con l'impiego di un normale sistema di videosorveglianza, sia perché l'elaborazione delle immagini per la verifica di eventuali camuffamenti non prevede la loro associazione ad altre immagini contenute in banche dati fotografiche.

Inoltre, da alcune banche sono pervenute anche richieste di verifica preliminare volte all'attivazione di un sistema comportante la rilevazione dei dati biometrici degli interessati per consentire alla clientela di accedere alle cassette di sicurezza -in modalità *self service*- 24 ore su 24 tutti i giorni della settimana. Il sistema sarebbe stato attivato, previo rilascio di apposito consenso informato, solo su specifica richiesta del cliente, con acquisizione di una sua impronta digitale attraverso un apposito lettore in grado di generare un algoritmo matematico univoco ed irripetibile, a sua volta memorizzato solo su una *smartcard* consegnata all'interessato unitamente ad un *pin*. Per i clienti che non avessero inteso avvalersi del sistema, sarebbero state previste modalità alternative di registrazione e di accesso al servizio di cassette di sicurezza, tramite l'inserimento di una carta magnetica e la digitazione del codice personale. All'esito dell'attività istruttoria, il Garante ha adottato singoli provvedimenti (provv. 13 settembre 2012 [doc. web n. 1927441] e provv. 18 ottobre 2012 [doc. web n. 2212554]) con i quali, nel ritenere lecita la finalità perseguita dalle banche e proporzionato il trattamento dei dati personali, ha prescritto agli istituti di credito l'adozione di specifici accorgimenti e, in particolare, di conservare una descrizione scritta dell'intervento effettuato dall'installatore, che attesti anche la conformità del sistema alle disposizioni del disciplinare tecnico (regola n. 25 dell'Allegato B. al Codice), nonché di notificare al Garante il trattamento dei dati biometrici prima dell'inizio delle operazioni di trattamento (art. 37, comma 1, lett. *a*), del Codice).

Con riferimento ad una ipotesi di cessione di ramo di azienda, l'Autorità si è espressa sull'istanza di una società operante nel settore del credito al consumo con la quale veniva

chiesto, in via principale, l'esonero dall'obbligo di rendere l'informativa agli interessati (tra cui, in particolare, i dipendenti e i clienti della società cedente) ed in via subordinata - considerata la particolare fattispecie della cessione del ramo di azienda- di poter rendere l'informativa con modalità semplificate, in particolare con quella prevista "*per la notizia della cessione dei rapporti giuridici in blocco, dall'art. 58 del testo unico delle leggi in materia bancaria e creditizia*". L'istanza rappresentava che le modalità ordinarie di informativa, per il numero elevatissimo di interessati (oltre 215.000 clienti), avrebbe comportato l'impiego di mezzi manifestamente sproporzionati.

L'Autorità, nel caso di specie, ha considerato che l'operazione negoziale intercorsa tra le due società (la suddetta cessione di ramo d'azienda) fosse regolata dall'art. 58, comma 7, del d.lgs. 1° settembre 1993, n. 385 (testo unico delle leggi in materia bancaria e creditizia T.u.b.) e -anche alla luce di un precedente provvedimento, in ragione della peculiarità della disciplina, della tipologia dei dati ceduti e dell'immutata finalità del trattamento- ha valutato come prevalente, rispetto alla riservatezza dei soggetti medesimi, l'interesse della società cedente alla comunicazione dei dati personali alla società cessionaria (v. art. 24, comma 1, lett. *g*), del Codice). Pertanto ha ritenuto che la comunicazione dei dati personali tra le due società potesse considerarsi lecita, anche in assenza del consenso degli interessati.

Di conseguenza, l'Autorità ha consentito alla società richiedente di rendere l'informativa agli interessati, contenente gli elementi previsti dall'art. 13, commi 1 e 2, del Codice, mediante la sua pubblicazione nella Gazzetta Ufficiale della Repubblica italiana, contestualmente alla pubblicazione dell'avviso di cessione "*in blocco*" dei rapporti giuridici previsto dall'art. 58 del T.u.b, prescrivendo altresì ad entrambe le società coinvolte, quali ulteriori "*misure appropriate*" (art. 13, comma 5, lett. *c*), del Codice), di pubblicare sui propri siti web un annuncio recante i contenuti dell'informativa (provv. 5 luglio 2012 [doc. web n. 1913790]).

14.2. SETTORE ASSICURATIVO

L'Autorità è stata chiamata a pronunciarsi su un'istanza di bilanciamento di interessi (art. 24, comma 1, lett. *g*), del Codice), presentata da alcune società appartenenti al medesimo

gruppo assicurativo e operanti nel ramo danni, in relazione al trattamento dei dati non sensibili dei molteplici soggetti (quali contraenti, danneggiati, periti, medici, legali, testimoni, carrozzieri) coinvolti, a vario titolo, nelle procedure di liquidazione dei sinistri. L'istanza -formulata nell'ambito di un progetto in fase di implementazione presso gran parte delle consociate europee finalizzato, tra l'altro, all'individuazione attraverso l'utilizzo di specifici modelli previsionali di possibili richieste di risarcimento danni fraudolente- avrebbe trovato fondamento, a detta delle società, nel loro legittimo interesse a tutelarsi contro fenomeni fraudolenti (oltre che nell'oggettiva impossibilità di acquisire un preventivo consenso da parte di tutti gli interessati), suffragata anche dalla normativa di settore. L'Autorità, nel riconoscere l'indubbia meritevolezza delle finalità perseguite, ha tuttavia accolto solo parzialmente l'istanza, ravvisando idonei presupposti per il richiesto bilanciamento esclusivamente in relazione ai soggetti coinvolti, a vario titolo, nelle procedure di risarcimento danni da responsabilità civile connessa alla circolazione di veicoli a motore; è stato precisato, tuttavia, che nulla osta, in linea di principio, a che le società trattino i dati personali degli interessati, per le finalità indicate e in relazione all'intero ramo danni, in presenza di altro presupposto di liceità di cui all'art. 24 del Codice (provv. 24 gennaio 2013 [doc. web n. 2352902]).

14.3. ALTRE ATTIVITÀ IMPRENDITORIALI

Nel 2012 il Garante ha intrapreso una importante attività di collaborazione con l'Autorità per l'energia elettrica e il gas in vista della realizzazione di una banca dati contenente i dati identificativi dei clienti delle imprese del settore, cd. "sistema informativo integrato", previsto da specifica normativa (art. 1-*bis*, l. 13 agosto 2010, n. 129, di conversione in legge, con modificazioni, del d.l. 8 luglio 2010, n. 105 recante "Misure urgenti in materia di energia"). Tale sistema è stato previsto a seguito della liberalizzazione del mercato dell'energia elettrica e del gas, che consente a tutti i clienti di scegliere liberamente il proprio fornitore. La banca dati, istituita presso Acquirente Unico S.p.A., ha soltanto lo scopo di risolvere il problema creato dal passaggio dei clienti da un fornitore all'altro in presenza di morosità pregresse (cd. "turisti energetici").