motori di ricerca il compito di contemperare libertà di informazione e diritto alla protezione dei dati appare problematico, tenuto conto che tali soggetti possono non sempre essere dotati degli strumenti di conoscenza necessari per effettuare le (talora complesse) valutazioni nei singoli casi. In questo senso, di particolare rilievo rimane il ruolo che le autorità di protezione dei dati personali o le autorità giudiziarie nazionali competenti dovranno svolgere per contribuire ad un effettivo bilanciamento dei due diritti.

A seguito dell'appena richiamata sentenza della Corte di giustizia, Google è tenuta a dare un riscontro alle richieste di cancellazione dai risultati della ricerca delle pagine web che contengono il nominativo del richiedente (cfr. in merito le linee guida sull'attuazione della sentenza della Corte di giustizia nel caso Google Spain adottate dal Gruppo Art. 29 il 26 novembre 2014). La società dovrà valutare di volta in volta vari elementi, quali l'interesse pubblico a conoscere la notizia, il tempo trascorso dall'avvenimento nonché l'accuratezza della notizia e la rilevanza della stessa nell'ambito professionale di appartenenza. Di fronte al diniego di Google, gli utenti italiani possono rivolgersi al Garante o all'autorità giudiziaria.

In base a questa procedura, il Garante ha adottato alcuni provvedimenti a seguito delle prime segnalazioni pervenute dopo il mancato accoglimento da parte di Google di richieste di deindicizzazione di pagine presenti sul web che riportavano dati personali ritenuti non più di interesse pubblico. Le segnalazioni e i ricorsi pervenuti al Garante hanno riguardato la richiesta di deindicizzazione di articoli relativi a vicende processuali ancora recenti e in alcuni casi non concluse. In sette dei nove casi definiti, il Garante non ha accolto la richiesta degli interessati, ritenendo che la decisione di Google fosse corretta, risultando prevalente l'interesse pubblico ad accedere alle informazioni tramite motori di ricerca, tenuto conto che le vicende processuali erano recenti e non erano stati espletati tutti i gradi di giudizio (cfr. provv.ti 6 novembre 2014, n. 496, doc. web n. 3623819; n. 497, doc. web n. 3623954; n. 498, doc. web n. 3623919; n. 499, doc. web n. 623851; n. 500, doc. web n. 3623897; n. 558, doc. web n. 3624003 e n. 557, doc. web n. 3624021).

In due casi, invece, il Garante ha accolto la richiesta dei segnalanti, dando prevalenza alla tutela del loro diritto alla protezione dei dati (provv. 22 dicembre 2014, n. 501, doc. web n. 3623877 e provv. 11 dicembre 2014, n. 581, doc. web n. 3623978). Nel primo, perché nei documenti pubblicati su un sito web erano presenti numerose informazioni eccedenti, riferite anche a persone estranee alla vicenda giudiziaria narrata. Nel secondo, perché la notizia pubblicata era inserita in un contesto idoneo a ledere la sfera privata della persona. Tutto ciò in violazione delle norme del Codice e del codice deontologico che impongono ai giornalisti di diffondere dati personali nei limiti dell'"essenzialità dell'informazione riguardo a fatti di interesse pubblico" e di non riferire abitudini sessuali riferite a una determinata persona identificata o identificabile. Il Garante ha quindi prescritto a Google di deindicizzare l'url segnalata.

Va evidenziato che sono alcune decine, al momento, le segnalazioni pervenute all'Autorità a seguito della sentenza della Corte di giustizia: un numero esiguo, se paragonato alle 15.000 istanze rivolte finora a Google da cittadini italiani con le quali è stata richiesta la rimozione di circa 50.000 url. Rimozioni che la società ha accolto per il 25% dei casi (v. sul punto il rapporto di Google rinvenibile all'indirizzo http://www.google.com/transparencyreport/removals/europeprivacy/?hl=it).

11 Il trattamento di dati personali attraverso internet

11.1. *Informativa e consenso per il trattamento dei dati personali mediante i siti web*

L'Ufficio ha ravvisato informative sul trattamento dati non del tutto idonee ai sensi dell'art. 13 del Codice rispetto ad alcuni siti web nonché, rispetto a *form* di registrazione a servizi vari, consensi non adeguatamente differenziati a seconda dei diversi trattamenti di dati personali indicati nei testi informativi ai sensi degli artt. 23 e 130 del Codice.

In materia si segnala l'adozione del provv. 25 settembre 2014, n. 427 (doc. web n. 3457687), dal contenuto inibitorio e prescrittivo, adottato in relazione alla ricezione di messaggi promozionali indesiderati via *e-mail* da parte di utenti che avevano prestato il proprio consenso al solo scopo di ottenere l'iscrizione ad un servizio di *newsletter online*.

11.2. *Il provvedimento prescrittivo nei confronti di Google Inc.*

Si è conclusa con un provvedimento a carattere prescrittivo (10 luglio 2014, n. 353, doc. web n. 3283078) una complessa e rilevante istruttoria che ha preso in esame la *privacy policy* adottata da Google Inc., con particolare riguardo al trattamento di dati personali effettuato per finalità di profilazione *online*. La decisione, adottata nell'ambito di un'azione coordinata con altre autorità di protezione dati europee, non si è limitata a richiamare la società statunitense al rispetto dei principi fissati dal Codice, ma ha anche indicato in concreto le misure e le modalità da adottare per rendere leciti i trattamenti effettuati, in particolare in materia di informativa, consenso e tempi di conservazione dei dati. In considerazione delle complessità, anche dal punto di vista tecnico, delle misure necessarie per dare attuazione alle prescrizioni, alla società è stato concesso un termine di diciotto mesi per l'adeguamento, nel corso del quale il Garante potrà monitorare tale processo avvalendosi di uno specifico protocollo di verifica concernente tempi e modalità dei controlli da parte dell'Autorità.

11.2.1. Google Street View Special Collects

Google Inc. ha comunicato all'Autorità l'intenzione di estendere al territorio nazionale un programma, già attivo altrove, di "raccolta immagini in luoghi unici e remoti, inclusi quelli con particolare valore naturalistico, storico e turistico", denominato *Google Special Collects*.

Al riguardo, ed in considerazione del campo di applicazione della raccolta di immagini in questione – riservata a luoghi (privati, pubblici ed aperti al pubblico) di particolare interesse artistico, turistico, storico e culturale che, per le loro caratteristiche strutturali, risultano accessibili esclusivamente a piedi o, comunque, con mezzi diversi dall'automobile –, l'Autorità, riconosciute le peculiarità del servizio rispetto alla versione *standard* di *Street View*, ha individuato adeguate cautele a tutela degli interessati e misure semplificate per informarli delle riprese (programmate o in corso). In particolare, Google dovrà rendere noti i luoghi oggetto di ripresa sul proprio sito web in italiano nei tre giorni antecedenti l'inizio delle riprese nonché, sette

giorni prima, anche sui siti web e, se esistenti, sulle *newsletter* o altre pubblicazioni informative dei *partners*, cioè degli enti, strutture, soggetti privati, fondazioni, ecc. coinvolti nel programma. Nei luoghi ad accesso controllato, Google o i suoi incaricati dovranno rendere nota alle persone interessate – anche attraverso appositi avvisi o cartelli affissi all'ingresso dei siti – l'imminente registrazione delle immagini, in modo da minimizzare il rischio per i visitatori che non lo desiderano di venire ripresi.

La società dovrà inoltre provvedere alla formazione del personale coinvolto circa il rispetto della normativa sulla protezione dei dati personali e dotare gli operatori di adesivi o altri segni distintivi chiaramente visibili da applicare sull'abbigliamento e sulle attrezzature, in modo da segnalare che si stanno acquisendo immagini da pubblicare *online* su *Google maps* mediante il servizio *Google Special Collects* nell'ambito di *Street View* (provv. 4 dicembre 2014, n. 555, doc. web n. 3633473).

11.3. *La raccolta dati* online *da siti specializzati per richieste di preventivi di prestiti*

Anche a seguito delle segnalazioni pervenute, l'Autorità ha avviato un'attività di verifica sul trattamento dei dati effettuati mediante siti web riferiti a consumatori nel settore delle domande di prestito personale e di altre modalità di finanziamento (in corrispondenza, ad esempio, della cd. cessione del quinto, dell'acquisto dell'auto o del "mutuo prima casa") con l'obiettivo di verificare la liceità dei trattamenti, anche alla luce delle Linee guida in materia di attività promozionale e contrasto allo *spam* (provv. 4 luglio 2013, n. 330, doc. web n. 2542348) ed il corretto impiego delle informazioni raccolte in sede di ricerca di possibili finanziamenti.

A seguito di tale attività il Garante ha adottato due provvedimenti inibitori e prescrittivi (provv.ti 9 ottobre 2014, n. 447, doc. web n. 3568046 e 20 novembre 2014, n. 532, doc. web n. 3657934). Nel primo caso, ha vietato ad una società di intermediazione *online* l'utilizzo dei dati personali dei clienti a fini di *marketing* in assenza di un loro consenso specifico. In particolare, a seguito di una segnalazione in cui si lamentava la ricezione di comunicazioni promozionali indesiderate, è stato accertato che la società sottoponeva agli utenti un modello di richiesta di consenso unico (ritenuto inidoneo), peraltro già pre-compilato nella casella relativa all'assenso, sia per la fornitura del servizio richiesto, sia per finalità diverse, quali l'invio di informazioni commerciali e la fidelizzazione della clientela. Il Garante ha inoltre prescritto di modificare e integrare l'informativa presente sul sito, al fine di rendere chiaramente noti agli utenti i trattamenti di dati effettuati, le modalità di svolgimento dell'attività promozionale per conto proprio o da parte di soggetti terzi nonché l'eventuale comunicazione a terzi dei dati.

Con il secondo provvedimento, valutate le informazioni presenti sul sito e previo accertamento *ex* art. 157 del Codice, il Garante ha dichiarato illecita e vietato la raccolta dei dati personali degli utenti effettuata da una società sul sito web per l'invio di comunicazioni promozionali per conto proprio e per conto terzi nonché di comunicazione dei dati raccolti a terzi per finalità promozionali (o comunque per finalità diverse da quelle strumentali ovvero collegate all'erogazione del servizio o all'esecuzione del contratto) senza aver provveduto alla previa acquisizione del necessario consenso libero e specifico degli interessati, oltre che informato e documentato per iscritto (art. 23, comma 3, del Codice); ha inoltre prescritto alla medesima società di modificare la formula di acquisizione del consenso nonché di specificare nell'informativa le modalità tradizionali (posta cartacea, telefonate con operatore) e/o automatizzate (posta elettronica, sms, fax) di utilizzazione dei dati per lo svolgimento dell'attività promozionale.

11.4. *L'attività istruttoria condotta dall'Autorità a seguito di accertamenti ispettivi del Nucleo speciale* privacy *e di segnalazioni*

È stata intensificata l'attività di verifica sulla conformità al Codice dei trattamenti effettuati da talune società editoriali in occasione della raccolta dei dati degli utenti sui rispettivi siti web; ciò con specifico riferimento all'informativa resa e alle modalità di acquisizione del consenso al trattamento dei dati (artt. 13, 23 e 130 del Codice) nonché ai fondamentali principi di finalità, necessità, proporzionalità e non eccedenza del trattamento (artt. 3-11 Codice). La complessa attività ha interessato principalmente editori oggetto di accertamenti ispettivi da parte del Nucleo speciale *privacy* della Guardia di finanza (nell'ambito del programma delle attività ispettive del primo semestre 2012) nei confronti dei quali erano stati individuati, già in sede ispettiva, profili di illiceità rispetto a taluni trattamenti determinando così l'avvio di procedimenti sanzionatori.

Tale approfondimento si è reso necessario in considerazione dell'abitualità della raccolta dei dati in questo ambito, spesso finalizzata al perseguimento di plurime finalità (consultare il giornale *online*; acquistare un abbonamento; ricevere *newsletter*; esprimere commenti sulle notizie, partecipare a *blog* e *forum* su temi di attualità) nonché considerata la complessità della struttura organizzativa dei titolari del trattamento (spesso strutturati in gruppi societari), con riflessi sull'ambito di circolazione nonché sulle modalità e finalità di utilizzo dei dati raccolti. L'Autorità ha quindi verificato non solo la "regolarizzazione" dei trattamenti alla luce delle contestazioni formulate in sede ispettiva, ma ha altresì esteso la verifica alle diverse attività di raccolta dei dati effettuate dagli editori attraverso i propri siti. Ciò anche alla luce dei provvedimenti generali in materia di *spam* (cfr. provv. 4 luglio 2013, n. 330, doc. web n. 2542346) e sul consenso al trattamento dei dati personali per finalità di *marketing* diretto (cfr. provv. 15 maggio 2013, n. 242, doc. web n. 2543820).

Fra i profili critici emersi si segnala che, nell'informativa e nello spazio dedicato all'acquisizione del consenso, tra le finalità ulteriori rispetto a quelle connesse alla prestazione del servizio richiesto, spesso è stato riscontrato il riferimento ad "attività statistiche e di sondaggio di opinioni" finalizzate anche a un "miglioramento del servizio richiesto". Tale formulazione ha reso necessario un chiarimento sulle effettive finalità (statistica aggregata/profilazione) perseguite dall'editore, essendo talvolta richiesti all'utente anche dati eccedenti rispetto a quelli necessari all'erogazione del servizio (di navigazione sul sito *web* o di accesso a determinati contenuti), in particolare con riferimento a dati concernenti professione, età, titolo di studio, sesso. Inoltre, in alcune informative è risultata mancare l'indicazione di un indirizzo *e-mail* dedicato all'esercizio gratuito e, per quanto possibile, agevole dei diritti di cui agli artt. 7 ss. del Codice, come suggerito dal Gruppo Art. 29 (cfr. parere n. 5/2004) e ribadito dalle citate Linee guida del 4 luglio 2013.

L'Autorità ha fatto presente a ciascun titolare che, in base all'art. 11, comma 2, del Codice, i dati personali raccolti in violazione della disciplina non avrebbero comunque potuto essere utilizzati per finalità promozionali, né avrebbero potuto essere comunicati a terzi per analoghe finalità, se non dopo aver raccolto un libero consenso informato e specifico per ciascuno di questi trattamenti, ai sensi degli artt. 13, 23 e 130 del Codice.

11.5. *L'utilizzo dei* cookie*: adozione del provvedimento generale*

Nella Relazione 2013 sono state descritte le modalità, improntate a criteri di ampia partecipazione, attraverso le quali l'Autorità ha acquisito, sia mediante consultazione pubblica sia mediante predisposizione di un apposito tavolo di lavoro, i contributi provenienti dalla comunità tecno-scientifica ed imprenditoriale sull'uso dei cd. *cookie* (i piccoli *file* di testo che i siti visitati dall'utente inviano al suo *browser* per essere poi ritrasmessi agli stessi siti alla successiva visita del medesimo utente) e di altri strumenti analoghi (quali *web beacon/web bug, clear* GIF). Ciò ha consentito di appurare che l'impiego dei *cookie* nell'ambito della navigazione in internet, se da un lato consente la profilazione degli utenti tesa all'invio di pubblicità mirata, dall'altro assicura anche il funzionamento dei servizi offerti *online*.

Alla luce degli elementi raccolti, con provvedimento generale dell'8 maggio 2014, n. 229 (doc. web n. 3118884), il Garante ha individuato modalità semplificate per rendere agli utenti l'informativa *online* e ha fornito indicazioni per acquisirne il consenso, quando richiesto, nonché per consentire agli interessati di decidere in maniera libera e consapevole se autorizzare l'uso delle informazioni personali inerenti la propria navigazione attraverso i siti visitati per ricevere pubblicità mirata. A maggior tutela degli utenti, il Garante ha stabilito che quando si accede alla *home page* o ad un'altra pagina di un sito web deve comparire un *banner* chiaramente visibile, in cui sia indicato:

- se il sito utilizza *cookie* di profilazione per inviare messaggi pubblicitari mirati;
- se il sito consente anche l'invio di *cookie* di "terze parti", ossia di *cookie* installati da un titolare del trattamento diverso rispetto a quello che gestisce il sito visitato;
- un *link* a una informativa più ampia, recante indicazioni sull'uso dei *cookie* inviati dal sito con le indicazioni necessarie a negare il consenso alla loro installazione direttamente o collegandosi ai vari siti nel caso dei *cookie* di "terze parti";
- l'indicazione che proseguendo nella navigazione (ad es., accedendo ad un'altra area del sito ovvero selezionando un'immagine o un *link*) si presta il consenso all'uso dei *cookie*.

Per quanto riguarda l'obbligo di tener traccia del consenso dell'utente, al gestore del sito è consentito utilizzare un *cookie* tecnico, in modo tale da non riproporre l'informativa breve alla seconda visita dell'utente, il quale conserva comunque la possibilità di modificare le proprie scelte sui *cookie* attraverso l'informativa estesa, che deve essere facilmente accessibile da ogni pagina del sito.

Il termine per l'implementazione delle misure prescritte è fissato per maggio 2015.

12 Il trattamento di dati personali nel settore delle comunicazioni elettroniche

12.1. *Il* telemarketing *"selvaggio"*

Per quanto riguarda le utenze iscritte al Registro pubblico delle opposizioni continua a pervenire un ingente numero di segnalazioni relative alla ricezione di chiamate promozionali indesiderate. Numerose segnalazioni hanno riguardato altresì telefonate a carattere commerciale effettuate nei confronti di utenze – fisse e mobili – non presenti negli elenchi telefonici (cd. utenze riservate) come pure di utenze, non riservate e non iscritte nel Registro pubblico delle opposizioni, per le quali è stato negato il consenso al trattamento dei dati personali nei confronti di una o più società (che, ciò nonostante, hanno effettuato le chiamate promozionali).

Parallelamente all'esame delle segnalazioni sono proseguite le complesse attività istruttorie volte ad individuare l'effettivo autore della chiamata indesiderata ed a riscontrare la presenza o meno di uno specifico consenso al trattamento dei dati personali da parte del segnalante. Il fenomeno delle chiamate indesiderate dirette a numeri presenti in elenco ha spesso comportato la necessità di acquisire informazioni direttamente dalla Fondazione Ugo Bordoni.

Sono ben 735 le comunicazioni – comprensive di richieste d'informazioni (anche *ex* art. 157 del Codice), richieste d'integrazione di istruttorie e note volte a verificare l'avvenuto adeguamento alla disciplina di protezione dei dati – inviate alle società segnalate od alla Fondazione Ugo Bordoni. Sono inoltre circa 100 le note inviate ai segnalanti per informarli sullo stato della propria pratica ovvero per richiedere informazioni integrative. In numerosi casi, peraltro, si è constatato che le aziende che hanno svolto attività a contenuto promozionale hanno operato anche tramite terzi i quali, a loro volta, hanno ulteriormente demandato l'attività promozionale ad altri soggetti, talora stabiliti all'estero. Lo svolgimento dell'attività istruttoria ha comportato altresì la necessità di svolgere un previo accertamento sulla titolarità delle utenze segnalate. In un sempre crescente numero di casi, tuttavia, il numero chiamante è risultato oscurato ovvero solo apparentemente in chiaro (in quanto, ricontattando l'utenza telefonica, la stessa è risultata essere "inesistente").

Sono state trattate un totale di 1.398 pratiche, delle quali, per più di 1.000, è stata conclusa l'attività istruttoria. In più di 80 casi, inoltre, l'attività è stata definita con la trasmissione degli atti al Dipartimento competente per l'apertura di un procedimento sanzionatorio. Gli accertamenti svolti nell'ambito delle istruttorie, peraltro, hanno determinato in taluni casi la necessità di effettuare attività di carattere ispettivo nei confronti sia dei soggetti committenti l'attività di *telemarketing*, sia di alcuni *call center* che le hanno materialmente poste in essere.

12.2. *Le nuove regole di contrasto alle telefonate mute effettuate da* call center *per finalità di* marketing

Il Garante ha continuato ad occuparsi del fenomeno delle chiamate mute, vale a dire delle telefonate promozionali nelle quali, a causa dell'arbitraria e non corretta

impostazione dei sistemi automatizzati di chiamata utilizzati dai *call center*, il destinatario, dopo aver risposto, non trova dall'altro capo del filo alcun operatore. Riguardo tale fenomeno, a seguito della consultazione pubblica avviata a fine novembre 2013, il Garante ha adottato il provvedimento 20 febbraio 2014, n. 83 (doc. web n. 3017499) indicando una serie di misure di contrasto. Con tale decisione, in particolare, si è stabilito che:

- i *call center* devono censire correttamente e secondo criteri uniformi le chiamate mute effettuate, che devono comunque essere interrotte entro un massimo di 3 secondi dalla risposta dell'utente;
- il numero di chiamate mute considerate entro la soglia di tollerabilità fisiologica non potrà essere superiore al 3% di tutte le chiamate andate a buon fine; tale percentuale dovrà essere misurata ad intervalli decadali e comunque nell'ambito di ogni singola campagna di *telemarketing*;
- alla risposta dell'utente non potrà far riscontro il silenzio, che dovrà invece essere sostituito da un rumore sintetico ambientale (cd. *comfort noise*), con rumori di sottofondo, squilli di telefono, brusio, ecc., per dare la sensazione che la chiamata non provenga da molestatori;
- a seguito di una chiamata muta, l'utente non potrà essere ricontattato prima di cinque giorni e comunque al contatto successivo dovrà essere prevista una modalità di instradamento automatico della chiamata in modo da assicurare la presenza di un operatore;
- i *call center* dovranno conservare per almeno due anni i *report* statistici delle chiamate mute effettuate, in modo da consentire gli opportuni controlli.

Il termine per l'adeguamento di sei mesi è scaduto il 2 ottobre 2014. Al riguardo, l'Autorità ha in programma di svolgere un'attività di carattere ispettivo al fine di verificare la conformità dei trattamenti di dati personali effettuati dai *call center* alle prescrizioni impartite.

12.3. *I trattamenti di dati personali effettuati mediante* call center *ubicati al di fuori dell'Unione europea*

A seguito delle prescrizioni impartite con il provvedimento del 10 ottobre 2013, n. 444 (doc. web n. 2724806), sono pervenute al Garante, da parte di quarantuno titolari del trattamento, le notificazioni di trasferimento o affidamento all'estero del trattamento di dati personali per servizi di *call center*. L'Autorità ha così potuto iniziare ad effettuare una ricognizione più completa del fenomeno acquisendo elementi utili a verificare la conformità alle prescrizioni impartite dal suddetto provvedimento ed alle disposizioni del Codice anche mediante accertamenti ispettivi, in collaborazione con il Nucleo speciale *privacy* della Guardia di finanza, per verificare la liceità dei trattamenti posti in essere dai titolari che si avvalgono di *call center* esteri.

12.4. *Dati personali utilizzati a fini di* marketing *e profilazione*

È stata presentata all'Autorità, ai sensi dell'art. 17 del Codice e del provvedimento generale del 24 febbraio 2005 relativo alle carte di fidelizzazione (doc. web n. 1103045), un'istanza di verifica preliminare da parte di una società che effettua crociere che aveva richiesto di poter conservare i dati della propria clientela per finalità di profilazione e *marketing* per un periodo pari a tredici anni rilevando che, per

poter effettuare una minima attività di profilazione, si sarebbe dovuto prendere in considerazione un numero di crociere sostenute dallo stesso passeggero pari a tre e che l'arco temporale indicato sarebbe stato congruo per tale finalità. Il Garante, con il provvedimento di accoglimento del 12 giugno 2014, n. 297 (doc. web n. 3315156), ricordando che tali attività necessitano comunque, preliminarmente, del consenso degli interessati, ha stimato congruo un periodo di conservazione massimo pari a dieci anni. Sempre con il medesimo provvedimento è stato altresì prescritto, allo scadere del suddetto termine di dieci anni, l'obbligo di cancellazione automatica dei dati conservati ovvero la trasformazione degli stessi in forma anonima in modo permanente.

Si deve evidenziare che, rispetto ai trattamenti svolti dai fornitori di servizi di comunicazione elettronica accessibili al pubblico per finalità di profilazione della propria clientela, attraverso l'uso di dati personali aggregati e senza l'acquisizione del previsto consenso specifico come stabilito nel provvedimento generale del 25 giugno 2009 (doc. web n. 1629107) e a seguito dei provvedimenti individuali emananti in tale ambito all'esito delle verifiche preliminari richieste da ciascun fornitore, il Garante ha adottato, a fronte di un'apposita istanza di riesame ed aggiornamento presentata da uno degli operatori telefonici coinvolti, uno specifico provvedimento prescrittivo (provv. 6 febbraio 2014, n. 54).

Al contempo, l'Autorità ha aggiornato le prescrizioni precedentemente impartite (provv. 6 febbraio 2014, n. 53, doc. web n. 2951718) rivedendo la misura prescrittiva che stabiliva un tempo di osservazione dei dati personali aggregati degli utenti per finalità di profilazione non inferiore ai trenta giorni. Ciò in virtù della prospettata esigenza, di fronte ad un nuovo assetto del mercato delle telecomunicazioni, di considerare, dopo alcuni anni dall'emanazione del provvedimento del 2009 e dei singoli provvedimenti prescrittivi, una nuova e più ridotta base temporale di aggregazione dei dati per finalità di profilazione, così da garantire un maggior equilibrio nei processi di gestione della clientela, soprattutto in ragione del crescente ricorso da parte degli utenti allo strumento della *number portability* e della crescente "offerta dati" legata alla diffusione di dispositivi radiomobili evoluti, quali *smartphone* e *tablet.*

In questo quadro il Garante ha previsto una riduzione del periodo di osservazione da un arco temporale mensile ad uno di due giorni, prescrivendo al contempo nuove cautele a garanzia degli utenti. Tra queste, l'Autorità ha disposto che la misurazione dei fenomeni che rilevano per l'attività di profilazione, sulla base di una aggregazione dei dati degli utenti relativa al suddetto arco temporale, debba riguardare esclusivamente: il volume di minuti in traffico originato o terminato (in minuti o *byte*); il numero di eventi di ricarica, distinto per canale di ricarica; il totale delle ricariche.

Limitatamente ai dati relativi al volume di minuti in traffico originato o terminato, il Garante ha inoltre previsto l'esclusione dall'impiego per finalità di profilazione dei periodi a cui corrisponda un solo evento di comunicazione elettronica riferibile ad un singolo utente.

Nel provvedimento si è altresì precisato che per tutte le altre misurazioni, ovvero per l'analisi aggregata dei dati che riguardano altri eventi che il fornitore individua per finalità di profilazione della clientela, quali i contatti dell'utente con il *customer care*, le visite ai diversi punti vendita ed assistenza del fornitore nonché le offerte relative ai terminali, la base temporale minima di riferimento debba essere di trenta giorni.

12.5. *I trattamenti dei dati personali per finalità di* marketing *diretto: manifestazione del consenso*

Nel caso di un noto gruppo societario l'Ufficio, dopo aver verificato che i dati del segnalante erano inseriti nelle liste dei soggetti contattabili per finalità di *marketing* diretto in assenza del necessario consenso, ha provveduto a trasmettere la relativa documentazione al competente Dipartimento ai fini dell'eventuale avvio di appositi procedimenti sanzionatori (nota 11 novembre 2014). In tale occasione si è ribadito che l'invio di comunicazioni pubblicitarie, anche con modalità automatizzate di contatto, deve essere effettuato nel rispetto delle norme che disciplinano i trattamenti in ambito privato a fini promozionali (artt. 23 e 130, commi 1 e 2, del Codice).

L'Autorità è intervenuta anche con riguardo ai profili della comunicazione a soggetti terzi e del trasferimento all'estero dei dati personali nell'ambito della stipula di contratti di assicurazioni per la responsabilità civile degli autoveicoli. In tali ipotesi è stato ribadito che, pur potendosi accettare l'acquisizione del consenso per finalità di *marketing* in calce al testo dell'informativa rilasciata al cliente e la successiva "premarcatura" in calce al contratto di assicurazione successivamente sottoscritto in quanto riproposizione di un consenso già rilasciato, non è invece da ritenersi ammissibile un consenso unico per finalità di *marketing* e di comunicazione a terzi (nota 23 dicembre 2014).

Il Garante è intervenuto in materia di manifestazione del consenso al trattamento per finalità promozionali anche con due provvedimenti inibitori e prescrittivi (provv. 9 gennaio 2014, n. 3, doc. web n. 2904350; provv. 25 settembre 2014, n. 427, doc. web n. 3457687). A seguito di segnalazioni inerenti alla ricezione di messaggi promozionali indesiderati via *e-mail*, l'Ufficio ha avviato altrettante istruttorie dalle quali è emerso che le stesse erano state inviate da società che avevano acquisito il consenso degli interessati in maniera non conforme al Codice, non essendo lo stesso libero e specifico.

In un caso infatti, la società titolare aveva raccolto il consenso al trattamento dei dati personali all'atto della sottoscrizione da parte dell'interessato di un modulo per l'attivazione della garanzia su un prodotto richiedendo un unico consenso per tutte le finalità (comprese quelle promozionali) indicate nella sua informativa; pertanto all'interessato non era lasciata la possibilità di esprimere liberamente la propria volontà in riferimento ad ogni distinta finalità di trattamento perché, in mancanza di consenso, non era possibile accedere al servizio. Nell'altro caso, invece, la stessa modalità di raccolta del consenso era stata utilizzata per richiedere l'iscrizione ad un servizio di *newsletter online*.

In entrambi i casi, il Garante, con i summenzionati provvedimenti, ha dichiarato illecito il trattamento effettuato per finalità promozionali poiché il consenso prestato dagli interessati non era libero e specifico ed ha vietato l'ulteriore trattamento dei dati così acquisiti avviando, al contempo, altrettanti procedimenti sanzionatori.

12.6. *Il* mobile payment

Facendo seguito all'attività conoscitiva svolta nel 2013 in merito ai nuovi servizi di pagamento attraverso il telefono cellulare, il Garante ha adottato, dopo una preliminare fase di consultazione pubblica (avviata il 12 dicembre 2013), un provvedimento generale in materia di trattamento di dati personali nell'ambito dei servizi di *mobile remote payment* (provv. 22 maggio 2014, n. 258, doc. web n. 3161560),

volto a delineare un primo quadro organico di regole, senza penalizzare lo sviluppo del mercato digitale.

Le misure previste hanno riguardato numerosi soggetti tra cui, in particolare, operatori di telecomunicazioni, *hub* tecnologici e fornitori di beni e servizi digitali fruibili tramite *smartphone*, *tablet* e *pc*, ma anche quanti offrono agli utenti la possibilità di acquistare, tramite applicazioni che consentono l'accesso a un mercato virtuale, contenuti digitali grazie al *mobile payment*. In questo ambito il provvedimento ha definito diversi profili, fra cui: le modalità per fornire l'informativa agli utenti e i suoi contenuti; le modalità per manifestare il consenso da parte degli interessati; la sicurezza e conservazione dei dati trattati.

In particolare, con riguardo all'informativa è stato chiarito che, oltre al richiamo alla finalità di erogazione del servizio attraverso la nuova modalità *mobile payment*, la stessa deve specificare se i dati personali dell'utente sono trattati anche per scopi ulteriori (quali *marketing* o profilazione) o comunicati a terzi, richiamando la necessità dell'acquisizione dell'apposito consenso dell'interessato.

In questo ambito, peraltro, sono state indicate le modalità di manifestazione del consenso, anche rispetto all'eventuale trattamento di dati sensibili. Infatti, il Garante ha evidenziato che, qualora dalla fruizione del contenuto o del servizio digitale sia possibile dedurre informazioni di natura sensibile, il consenso dell'interessato deve essere manifestato per iscritto, ovvero con altra modalità telematica equiparabile allo scritto, nel rispetto di quanto previsto dall'art. 26, comma 1, del Codice. Nella medesima ottica, la modalità telematica equiparabile allo scritto può implicare, oltre al ricorso ad un documento sottoscritto con firma elettronica qualificata o digitale, anche il ricorso a forme alternative più diffuse, secondo quanto previsto dal menzionato d.P.R. n. 445/2000. In ogni caso è possibile per il titolare del trattamento individuare forme alternative di manifestazione del consenso in luogo di quelle previste dalla normativa, soggette alla valutazione del Garante ai sensi dell'art. 17 del Codice.

L'Autorità ha prescritto nuove misure volte a garantire la sicurezza dei dati, quali sistemi di autenticazione forte per l'accesso ai dati da parte del personale, procedure di tracciamento degli accessi e delle operazioni effettuate, criteri di codificazione dei prodotti e servizi, forme di mascheramento dei dati.

Altre misure sono state individuate anche al fine di evitare i rischi di una integrazione tra le diverse tipologie di dati a disposizione dell'operatore telefonico (consumo/traffico telefonico e dati relativi alla fornitura di altri beni digitali, quali ad esempio quelli legati alla cd. tv interattiva) e impedire quindi un'eventuale profilazione incrociata dell'utenza rispetto alle abitudini, ai gusti ed alle preferenze di consumo, in assenza del relativo consenso espresso, specifico e informato.

Anche per i *merchant* (i fornitori di contenuti digitali offerti agli utenti, quali copie digitali di quotidiani, *social games*, *e-book*, contenuti musicali e video), nella prospettiva di garantire la maggiore riservatezza dei dati dei clienti, è stata prevista la trasmissione all'operatore telefonico delle sole categorie merceologiche di riferimento dei prodotti digitali offerti, senza indicazioni sullo specifico contenuto del prodotto o servizio acquistato, a meno che ciò non sia in concreto necessario per la fornitura di servizi in abbonamento.

Altri accorgimenti hanno riguardato la previsione di apposite misure di sicurezza per la fruizione di servizi destinati ad un pubblico adulto, nonché la conservazione dei dati trattati.

Successivamente, in accoglimento dell'istanza interpretativa e di riesame di alcune prescrizioni contenute nel provvedimento suindicato presentata da un'associazione rappresentativa del settore e della successiva istanza di proroga del termine di attuazione previsto dal provvedimento stesso, l'Autorità (cfr. provv. 20 novembre 2014,

n. 546, doc. web n. 3610915) ha prorogato il termine al 31 marzo 2015, fornendo altresì indicazioni interpretative (classificazione dei contenuti; misure di sicurezza; periodo di conservazione dei dati).

12.7. *Il contrasto allo* spam

Numerose continuano ad essere le segnalazioni relative a sms, fax e (ancor più) *e-mail* indesiderati: nel coltivarle, non di rado risulta difficile individuare i titolari del trattamento, per le modalità con cui si può operare in rete, sia perché talora i siti mittenti risultano intestati a soggetti di fantasia o comunque privi di recapiti utilmente contattabili, sia perché spesso essi hanno sede in Paesi (anche extraeuropei) ove l'Autorità non ha competenza (v. art. 5 del Codice).

Al riguardo va però ribadito che l'attività di contrasto al fenomeno dello *spam* proveniente dall'estero incontra ancora ostacoli a causa di alcune differenze tra le legislazioni degli Stati europei, non solo in termini di disciplina sostanziale ma anche per quanto attiene alle tutele azionabili, con particolare riferimento alla tipologia di soggetti tutelati dagli ordinamenti in questo specifico ambito (persona fisica; persona giuridica; enti; associazioni). Differenze che, si auspica, verranno eliminate o comunque attenuate dal nuovo regolamento UE in materia di protezione dei dati personali, almeno riguardo a profili essenziali (quali i soggetti aventi diritto alle tutele previste dalla normativa in materia di protezione dei dati; i diritti tutelabili presso le Autorità nazionali preposte; i criteri di raccordo fra le competenze di tali Autorità, per trattamenti di dati che interessino più ordinamenti nazionali).

Con riguardo ai fax indesiderati si segnala il provvedimento del 23 gennaio 2014, n. 30 (doc. web n. 2927848), a tutela delle persone giuridiche, il quale ha ribadito che le disposizioni normative del capo 1 del titolo X del Codice, e in particolare quelle sulle modalità automatizzate di contatto promozionale (*e-mail*; *sms*; fax; *mms*; telefonate preregistrate), poiché riguardano i "contraenti", tutelano non solo le persone fisiche ma anche persone giuridiche, enti e associazioni. Quindi, ad ordinamento vigente, i titolari del trattamento dei dati relativi ai detti soggetti sono sottoposti al potere dell'Autorità di intervenire anche *ex officio* nonché all'applicazione delle sanzioni ammnistrative e penali previste dal Codice (e, tra queste, dall'art. 162, comma 2-*bis*) (v. provv. 20 settembre 2012, doc. web n. 2094932, e, analogamente, punto 2.2, Linee guida 4 luglio 2013, n. 330, doc. web n. 2542348). Peraltro, è stato chiarito che sono "dati personali" anche quelli relativi a professionisti e ad alcune imprese, come ad esempio per le persone fisiche che gestiscono ricevitorie o tabaccherie o agenzie di viaggio, in quanto tali soggetti sono da ritenersi "interessati" ai sensi dell'art. 4 del Codice. Inoltre, è stato precisato che l'invio di un fax è già in sé un trattamento di dati personali, indipendentemente dall'eventuale successivo inserimento dei dati del destinatario in un elenco *online* o comunque accessibile al pubblico, che costituisce un ulteriore distinto trattamento; dal numero dei fax eventualmente inviati al destinatario della promozione, bastando anche un solo fax indesiderato per integrare un trattamento di dati illegittimo; dall'informativa sul trattamento resa al destinatario ai sensi dell'art. 13 del Codice; dall'avviso del titolare ai destinatari delle promozioni indesiderate riguardo ai diritti di cui agli artt. 7 ss. del Codice; dal fatto che i dati in questione vengano cancellati subito dopo l'invio indesiderato in caso di mancata risposta o di opposizione dei destinatari. È stato ribadito che, senza il consenso libero e specifico dell'interessato, non è possibile trattare i dati "tratti da registri pubblici, elenchi, siti web, atti o documenti conosciuti o conoscibili da chiunque" (v. punto 2.5, Linee guida 4 luglio 2013).

12.8. *Servizi di TV digitale: non è* spam

È stata esaminata una segnalazione che lamentava la ricezione di messaggi pubblicitari indesiderati, associati alla visione di programmi offerti da un operatore telefonico nell'ambito dei servizi di tv digitale, che non sono assimilabili alle modalità di contatto automatizzato di cui all'art. 130, commi 1 e 2, del Codice.

Al riguardo, tuttavia, è emerso che i messaggi di cui si lamentava la ricezione non avevano natura pubblicitaria, trattandosi di *video-clip* di breve durata tesi esclusivamente ad informare l'utente circa i contenuti audiovisivi disponibili, a cui l'apposito *decoder*, installato per la ricezione del servizio televisivo digitale terrestre, consentiva l'accesso, nonché la possibilità per l'utente di bloccare tale ricezione attraverso due diverse modalità funzionali. In considerazione di ciò, l'Ufficio non ha ravvisato i presupposti per l'applicabilità della normativa sulla protezione dei dati personali.

12.9. *Le notificazioni di avvenuti* data breach

Sono pervenute all'Autorità ventidue comunicazioni di *data breach*, formulate dai più importanti fornitori di servizi di comunicazione elettronica operanti in Italia. La maggior parte delle violazioni notificate ha riguardato la perdita accidentale di documentazione contrattuale pur essendo sempre presente una copia dei dati in formato elettronico acquisita sui sistemi dei titolari. In alcuni casi, la violazione ha riguardato i servizi offerti *online* dai fornitori sui propri siti web, come quelli che consentono ai clienti di effettuare ricariche telefoniche o visualizzare il traffico telefonico effettuato a fini di controllo dell'esattezza degli addebiti. Gli incidenti hanno determinato la visualizzazione, da parte di alcuni clienti, dei dati relativi ad altri interessati.

In tali vicende, l'Autorità, all'esito delle istruttorie svolte nei confronti dei fornitori, ha verificato che fossero state adottate misure idonee a porre rimedio alle violazioni subite e a prevenirne di analoghe assicurandosi, al contempo, che gli interessati fossero stati informati dagli operatori nei casi previsti. Non si è ritenuto necessario adottare uno specifico provvedimento; in un solo caso la violazione non è stata prontamente notificata dalla società per difetto di qualificazione del reclamo ricevuto da un cliente il quale però, nel frattempo, aveva segnalato l'evento al Garante e dato impulso ad un'apposita istruttoria; è stato così rilevato il mancato rispetto, da parte del fornitore, dei ristretti termini previsti per la comunicazione al Garante (24 ore dall'avvenuta conoscenza della violazione per la prima sommaria comunicazione e 3 giorni da questa per la comunicazione dettagliata) ed è stato avviato un separato procedimento sanzionatorio.

Accanto alla gestione ordinaria delle comunicazioni di *data breach*, l'Autorità ha seguito gli approfondimenti svolti a livello europeo, partecipando ad una serie di incontri con le altre autorità competenti in ambito comunitario. I temi di maggiore rilievo affrontati hanno riguardato la collaborazione tra le diverse autorità nazionali competenti, la valutazione delle misure tecnologiche di protezione adottate dai fornitori, con particolare riferimento all'inintelligibilità dei dati, per far fronte alle singole violazioni e l'introduzione di eventuali ipotesi di esenzione dall'obbligo di notificazione.

12.10. Data retention

È proseguita l'analisi delle risultanze del ciclo ispettivo effettuato dal Nucleo speciale *privacy* in materia di conservazione di dati di traffico telefonico e telematico (cfr. Relazione 2013, *passim*), come noto oggetto della sentenza della Corte di giustizia dell'8 aprile 2014 (Digital Rights Ireland e Seitlinger e a., cause riunite C-293/12 e C-594/12) con la quale la Corte ha dichiarato invalida la direttiva sulla conservazione dei dati di traffico ritenendo che dalla stessa derivi un'ingerenza di ampia portata e di particolare gravità nei diritti fondamentali al rispetto della vita privata e alla protezione dei dati (cfr. par. 23.3).

Tali accertamenti, avviati nel 2012 a seguito di delibera del Collegio, erano stati effettuati nei confronti di vari fornitori di comunicazione elettronica accessibili al pubblico di piccole e medie dimensioni. Ciò al fine di verificare il rispetto delle prescrizioni impartite dal Garante con il provvedimento generale del 17 gennaio 2008 concernente la sicurezza dei dati di traffico telefonico e telematico, successivamente integrato con un secondo provvedimento generale del 24 luglio 2008, resosi necessario in virtù del recepimento della direttiva 2006/24/CE (cd. direttiva Frattini), riguardante "la conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione", avvenuto con il d.lgs. 30 maggio 2008, n. 109, che ha modificato, tra l'altro, l'art. 132 del Codice (cfr. doc. web nn. 1482111 e 1538237).

All'esito di tale attività è stato adottato il provv. 20 febbraio 2015, n. 84 (doc. web n. 3031194) grazie al quale è stata prescritta al fornitore l'adozione di specifici sistemi di autenticazione informatica, fondati su tecniche di *strong authentication*, di cui una necessariamente basata sull'elaborazione di caratteristiche biometriche dell'incaricato, nonché la tenuta di un apposito registro degli accessi. È stato altresì prescritto di svolgere, con cadenza almeno annuale, un'attività di controllo interna adeguatamente documentata e di procedere, entro il medesimo termine, alla cancellazione dei dati di traffico relativi alle chiamate senza risposta conservati oltre il termine di trenta giorni previsto dall'art. 132, comma 1-*bis*, del Codice.

13 La protezione dei dati personali nel rapporto di lavoro pubblico e privato

Il trattamento dei dati personali connesso all'attuazione delle discipline in materia di trasparenza amministrativa, oggetto delle "Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati" (provv. 15 maggio 2014, n. 243, doc. web n. 3134436), è stato uno dei profili sui quali si è focalizzata l'attenzione del Garante in ambito lavorativo; ma non può non rilevarsi il persistere di un significativo interesse per la materia della videosorveglianza in relazione alla quale l'Autorità è stata investita da numerose istanze di intervento. L'ambito di utilizzo delle tecnologie di localizzazione nel contesto lavorativo si è andato estendendo anche ai dispositivi mobili quali gli *smartphone* forniti in dotazione ai dipendenti: in particolare il Garante è stato chiamato a pronunciarsi sulle condizioni di liceità delle applicazioni informatiche che consentono la localizzazione dei lavoratori.

Rappresentatività sindacale nel settore privato

Con riguardo al tema della misura della rappresentatività sindacale nel settore privato, ai fini della contrattazione nazionale di categoria, di particolare rilievo il parere reso su richiesta dell'Istituto nazionale della previdenza sociale (Inps) avente ad oggetto uno schema di convenzione tra l'Istituto e Confindustria, Cgil, Cisl e Uil al fine di verificare la rappresentatività dei sindacati, così come previsto dal "Testo unico sulla rappresentanza" sottoscritto il 10 gennaio 2014. Esaminata la bozza di convenzione, l'Autorità ha sottolineato che, per misurare la rappresentatività sindacale, non è necessaria la trasmissione da parte delle imprese all'Inps dei dati sensibili, concernenti l'affiliazione sindacale, riferiti a ciascun lavoratore, in quanto lo stesso fine è perseguibile mediante la sola rilevazione del mero numero di deleghe assegnate a ciascuna sigla sindacale (parere 18 dicembre 2014, n. 609, doc. web n. 3721603). In linea con quanto espresso dal Garante, in data 16 marzo 2015 è stata quindi stipulata la menzionata convenzione nella quale si prevede la raccolta da parte dell'Inps dei soli dati numerici concernenti le deleghe riferite a ciascuna sigla sindacale. Tali dati numerici saranno successivamente trasmessi al Cnel per lo svolgimento delle operazioni di ponderazione e di determinazione della misura della rappresentatività di ciascuna sigla sindacale stipulante la convenzione.

13.1. *Il trattamento di dati personali e i controlli a distanza*

Videosorveglianza

L'esame della casistica che ha formato oggetto di provvedimenti collegiali in materia di rapporti di lavoro, anche a seguito di accertamenti ispettivi, conferma che in relazione all'utilizzo di strumenti di controllo, in particolare di sistemi di videosorveglianza, si riscontra un'area significativa di trattamenti non conformi, oltre che alla disciplina di settore (art. 4, l. n. 300/1970), anche alla disciplina sul trattamento dei dati personali (artt. 11, comma 1, lett. *a*), e 114 del Codice).

L'inosservanza della disciplina vigente in materia è stata accertata, unitamente alla violazione delle disposizioni che impongono di informare compiutamente sia i dipendenti che i terzi (in particolare clienti e fornitori) circa le caratteristiche essenziali dei sistemi di videosorveglianza installati, in relazione a titolari del trattamento

che svolgono attività eterogenee, in particolare quella relativa al settore alberghiero (provv. 9 gennaio 2014, n. 13, doc. web n. 2927804), alla grande distribuzione (provv. 8 maggio 2014, n. 230, doc. web n. 3250490) e ai piccoli esercizi commerciali (provv.ti 18 settembre 2014, n. 412, doc. web n. 3500271 e 4 dicembre 2014, n. 559, doc. web n. 3671057).

È stata altresì riscontrata l'inosservanza dell'obbligo di effettuare la designazione degli incaricati del trattamento e, in caso di affidamento dei servizi di vigilanza a soggetti esterni (svolti, ad es., tramite accesso alla *control room* dove vengono visualizzate in tempo reale le immagini raccolte con le telecamere di sorveglianza oppure mediante installazione di sistemi di allarme gestiti da remoto contestualmente al monitoraggio delle immagini), della designazione di questi ultimi quali responsabili del trattamento (provv.ti 9 gennaio 2014, n. 13 e 4 dicembre 2014, n. 559, cit.). Tali adempimenti, previsti dagli artt. 29 e 30 del Codice, sono finalizzati individuazione di soggetti realmente idonei a trattare i dati personali conformemente alla disciplina vigente, in base alle specifiche istruzioni predisposte dal titolare del trattamento.

Il Garante ha anche precisato che i dati personali riferiti ai dipendenti trattati attraverso un sistema di videosorveglianza installato per finalità di sicurezza e di tutela dei beni aziendali non possono essere utilizzati per contestare illeciti disciplinari (provv. 2 ottobre 2014, n. 434, doc. web n. 3534543). Tale utilizzo per scopi ulteriori e diversi rispetto a quelli originariamente perseguiti si pone in contrasto sia con il principio di finalità del trattamento (art. 11, comma 1, lett. *b*), del Codice) che con la disciplina vigente in materia di controlli a distanza dei lavoratori (cfr. provv. 8 aprile 2010, doc. web n. 1712680, punto 4.1; v. in merito anche le puntualizzazioni formulate a seguito di una verifica preliminare relativa ad un sistema di videosorveglianza cd. intelligente presso la Banca d'Italia riferite al par. 4.8).

Si segnala inoltre che l'Autorità – in occasione della richiesta avanzata da una società del settore metalmeccanico – ha chiarito che l'installazione di telecamere all'interno degli spogliatoi aziendali viola i principi di liceità, necessità, pertinenza e non eccedenza (posti dagli artt. 3 e 11, comma 1, lett. *a*), del Codice). Infatti all'interno di tali aree l'intimità e la dignità dei dipendenti devono essere indefettibilmente tutelate, anche alla luce delle vigenti disposizioni dell'ordinamento civile e penale, come già affermato in precedenza (provv. 10 luglio 2014, n. 357, doc. web n. 3325380).

Geolocalizzazione

Quanto all'utilizzo delle tecnologie di localizzazione in ambito lavorativo, tema già oggetto di un provvedimento di carattere generale con riferimento alla geolocalizzazione di veicoli (provv. 4 ottobre 2011, n. 370, doc. web n. 1850581), il Garante si è pronunciato sulle condizioni di liceità dell'utilizzo di applicazioni informatiche che consentono di localizzare geograficamente dispositivi mobili (*smartphone*) forniti in dotazione ai dipendenti. In particolare, nell'ambito di verifiche preliminari richieste da due importanti società di telecomunicazioni, l'Autorità ha ritenuto che il trattamento di dati personali riferiti alla localizzazione di dispositivi che – differentemente dai veicoli di servizio – da un lato "seguono" costantemente il dipendente, dall'altro si prestano ad utilizzi anche privati (nel caso considerato, peraltro, consentiti dal datore di lavoro), presenta rischi specifici per le libertà (ad es., di circolazione e di comunicazione), i diritti e la dignità dei lavoratori (v. provv.ti 11 settembre 2014, n. 401, doc. web n. 3474069 e 9 ottobre 2014, n. 448, doc. web n. 3505371). L'utilizzo dei sistemi – finalizzato al perseguimento di finalità organizzative e di sicurezza del lavoro nonché configurato in modo tale da non consentire la rilevazione continuativa dei dati – è stato pertanto subordinato all'adozione di misure di tipo organizzativo e tecnologico volte ad impedire l'eventuale trattamento da parte del datore di lavoro di informazioni presenti sul dispositivo estranee alla finalità di gestione del rapporto di lavoro (ad es., riferite a sms, traffico telefonico, posta elettronica, naviga-

zione in internet) e a rendere edotti i dipendenti in tempo reale (attraverso un'apposita icona sullo schermo dello *smartphone*) dell'attivazione della funzionalità di localizzazione. È stata data inoltre applicazione alla disciplina sul cd. bilanciamento di interessi (cfr. art. 24, comma 1, lett. *g*), del Codice), considerato anche che i titolari del trattamento hanno attivato le procedure previste dalla disciplina in materia di controlli a distanza dei dipendenti (previste dall'art. 4, comma 1, l. n. 300/1970) ed hanno dichiarato che i dati relativi alla posizione geografica non verranno utilizzati per finalità disciplinari.

Anche in relazione ai dati relativi alla posizione geografica, come nell'ambito della videosorveglianza, il Garante ha ritenuto che l'eventuale utilizzo per fini disciplinari di sistemi installati per scopi organizzativi, produttivi o legati alla sicurezza del lavoro non sarebbe conforme sia al principio di finalità del trattamento (art. 11, comma 1, lett. *b*), del Codice) che alla disciplina vigente in materia di controlli a distanza dei lavoratori, anch'essa applicabile (provv. 2 ottobre 2014, n. 434, cit.).

13.2. *Il trattamento di dati personali nella gestione del rapporto di lavoro*

L'Autorità continua a ricevere numerose segnalazioni e reclami relativi a forme di accesso ad informazioni personali oppure a modalità di circolazione delle stesse all'interno della struttura lavorativa, ritenute indebite, tanto nel settore pubblico che nel settore privato.

A tale proposito il Garante, nel confermare che il personale che svolge specifiche mansioni di segreteria in base ad un atto di preposizione può legittimamente curare la consegna di comunicazioni al dipendente di una amministrazione pubblica (nel caso specifico con qualifica dirigenziale) nell'ambito di un procedimento disciplinare, quanto alle modalità di consegna delle stesse ha ritenuto altresì lecito l'utilizzo dell'indirizzo di posta elettronica istituzionale assegnato al dipendente contestualmente alla consegna a mano in busta chiusa (all'interno della stanza assegnata al dipendente stesso). È stata invece ritenuta non conforme al principio di pertinenza e non eccedenza l'invio di copia di una contestazione disciplinare ad una articolazione interna dell'ufficio sprovvista di competenze relative al procedimento disciplinare (provv. 31 luglio 2014, n. 392, doc. web n. 3399423).

In un altro caso, con riguardo al trattamento dei dati personali dei dipendenti posto in essere da un gestore del servizio di trasporto pubblico, consistente nella affissione sulle bacheche ubicate presso i depositi aziendali (nonché tramite la rete aziendale intranet), di tabelle relative ai turni di servizio degli autisti, il Garante ha chiarito che sebbene le informazioni concernenti le causali di assenza dei lavoratori possano lecitamente essere oggetto di trattamento da parte del datore di lavoro – mediante il personale espressamente incaricato ai sensi dell'art. 30 del Codice –, nella misura in cui siano necessarie e pertinenti per dare corretta esecuzione al rapporto di lavoro ovvero per attuare previsioni contenute in leggi, regolamenti, contratti e accordi collettivi (artt. 11 comma 1, lett. *a*) e *d*), nonché 24, lett. *a*) e *b*) e, con riferimento ai dati sensibili, art. 26 del Codice e autorizzazione n. 1/2013, relativa al trattamento dei dati sensibili nei rapporti di lavoro) tuttavia, le medesime informazioni, specie se di natura sensibile, non possono essere messe a conoscenza di terzi non legittimati e degli altri dipendenti addetti al servizio di trasporto. Il Garante, sebbene non abbia ritenuto sussistente nel caso di specie, un'ipotesi di diffusione ai sensi dell'art. 4, comma 1, lett. *m*), del Codice – atteso che le tabelle erano state rese disponibili al personale in una sezione ad accesso riservato della intranet aziendale e su bacheche ubicate in locali il cui accesso era consentito unicamente ad