geolocalizzazione dello *smartphone* dei dispersi a una centrale operativa dedicata del Cnsas, senza l'intermediazione dell'operatore telefonico e il consenso delle persone da soccorrere.

Il citato parere è stato espresso anche alla luce di quanto già stabilito nel provvedimento 19 dicembre 2008 (doc. web n. 1580543) e fatte salve alcune condizioni: che i dati raccolti dal Cnsas riguardino esclusivamente la posizione geografica del terminale della persona dispersa o infortunata e non i dari relativi al traffico o altre tipologie di dati eccedenti o non pertinenti; tali dati siano utilizzati dal Cnsas soltanto per lo scopo di salvaguardare la vita o l'integrità fisica delle persone disperse o infortunate e, pertanto, solo quando siano state attivate formalmente le ricerche di tali soggetti; i medesimi dati siano raccolti da parte del personale del Cnsas appositamente incaricato ai sensi dell'art. 30 del Codice; tali tecnologie siano attivate sull'apparecchio della persona dispersa o infortunata in modo da abilitare le funzionalità di trasmissione delle coordinate gps, ovvero l'invio di sms contenenti le coordinate delle stazioni radio base visibili dal terminale, unicamente per il tempo necessario alla localizzazione del terminale (provv. 22 gennaio 2015, n. 32, doc. web n. 3736199).

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

Il Garante ha seguìto le importanti innovazioni della disciplina laburistica introdotte dai decreti legislativi attuativi della l. n. 183/2014 (cd. *Jobs Act*) ed in particolare la novella dell'art. 4, l. n. 300/1970 introdotta con il d.lgs. n. 151/2015, che modifica, in modo significativo, la regolazione dei controlli a distanza dei lavoratori. L'Autorità ha espresso la propria posizione nel corso dei lavori parlamentari in sede di audizioni del Presidente da parte delle Commissioni lavoro della Camera e del Senato, avvenute rispettivamente il 9 e il 14 luglio 2015 (doc. web n. 4119045).

I provvedimenti adottati dal Garante in questo ambito nel 2015 si riferiscono, peraltro, a casi rispetto ai quali trovava applicazione la disciplina previgente e confermano che, in relazione all'utilizzo di strumenti che consentono il controllo a distanza dei dipendenti, si riscontra un'area significativa di trattamenti non conformi alla disciplina sul trattamento dei dati personali.

Il Garante è altresì intervenuto in merito al trattamento di dati biometrici dei lavoratori per finalità di sicurezza, al trattamento di dati personali nella gestione del rapporto di lavoro, con particolare riguardo alla comunicazione all'esterno di dati relativi a lavoratori, alla loro pubblicazione e alle possibili interferenze con la disciplina in materia di trasparenza.

12.1. *I controlli a distanza mediante videosorveglianza*

Obbligo di informativa

In relazione all'utilizzo di sistemi di videosorveglianza nell'ambito del rapporto di lavoro, anche nel 2015 sono state accertate violazioni della disciplina applicabile in materia di protezione dei dati, in particolare dell'obbligo di informare con modalità adeguate gli interessati in ordine alle caratteristiche dei sistemi adottati nonché dell'obbligo di conformarsi a quanto prescritto dalla disciplina di settore in materia di controlli a distanza.

All'esito di accertamenti ispettivi disposti presso le sedi di una Provincia, l'Autorità ha, pertanto, dichiarato l'illiceità di un sistema di videosorveglianza in relazione al quale non si era provveduto ad apporre i prescritti cartelli informativi in prossimità del raggio di azione delle telecamere né era stata fornita adeguata informativa ai dipendenti. È emerso, inoltre, che l'ente non aveva provveduto ad attivare la procedura di garanzia prevista dall'art. 4, l. 20.5.1970, n. 300 (provv. 30 luglio 2015, n. 455, doc. web n. 4261028).

Allungamento tempi di conservazione

Il Garante ha, inoltre, esaminato alcune istanze di verifica preliminare volte ad ottenere la conservazione delle immagini raccolte attraverso sistemi di videoripresa oltre il termine massimo di sette giorni individuato in termini generali, in applicazione del principio di proporzionalità del trattamento, dal provvedimento in materia di videosorveglianza (provv. 8 aprile 2010, doc. web n. 1712680, v. punto 3.4).

In tutti i casi esaminati (quattro) l'Autorità ha riconosciuto l'esistenza, in concreto, di speciali esigenze di ulteriore conservazione da parte dei titolari del trattamento, legare a particolari esigenze di sicurezza di persone e/o di beni in relazione alle specifiche attività svolte. I soggetti richiedenti, che operano nel settore della produzione farmaceutica, dell'esazione dei pedaggi autostradali e dell'organizzazione e

gestione di manifestazioni fieristiche di beni di valore, hanno prospettato termini di conservazione ritenuti nel complesso congrui (rispettivamente 60, 20 e 10 giorni).

Del tutto peculiare è stata l'istanza di verifica preliminare presentata dalla Banca d'Italia in relazione all'attività di produzione, confezionamento e distruzione di banconote euro e di carta filigranata, posto che le relative condizioni di sicurezza (compresi i termini di conservazione per 12 mesi delle immagini raccolte) sono disciplinate da puntuali decisioni della Banca centrale europea, dotate di efficacia vincolante nei confronti dell'istituto di emissione.

Il Garante ha, altresì, ritenuto conformi al principio di proporzionalità le concrete modalità dei prospettati trattamenti, all'esito di una valutazione che ha riguardato, ad esempio, la limitazione dell'angolo di ripresa delle telecamere o l'indicazione di limiti all'accessibilità delle immagini conservate. In proposito si segnala anche che, in relazione all'attività di esazione dei pedaggi, la società richiedente si è impegnata ad adottare specifiche cautele, affinché pure i dipendenti di soggetti terzi che effettuano servizi di vigilanza siano preventivamente ed adeguatamente informati circa le caratteristiche del sistema di videosorveglianza installato.

In tutti i casi, infine, l'Autorità ha verificato che fosse stata rispettata la disciplina di settore applicabile in materia di controlli a distanza dei dipendenti (provv.ti 8 gennaio 2015, n. 4, non pubblicato ai sensi dell'art. 24 del reg. Garante 1° agosto; 12 marzo 2015, n. 142, doc. web n. 3822691; 8 luglio 2015, n. 413, doc. web n. 4253008; 17 settembre 2015, n. 476, doc. web n. 4360913).

Videosorveglianza "mobile"

Sistemi di videosorveglianza sono utilizzati, sempre più di frequente, da Forze di polizia locale nell'ambito del perseguimento delle funzioni istituzionali individuate dall'ordinamento.

In relazione a tale fenomeno il Garante, in un caso particolare, ha ritenuto illeciti i trattamenti di dati personali effettuati da un consorzio di polizia locale sia attraverso l'adozione di un sistema di videosorveglianza "mobile" operante sul territorio dei comuni aderenti al consorzio - con l'installazione sulle macchine di servizio di telecamere collocate in modo da riprendere la parte anteriore del veicolo, la carreggiata e il marciapiedi - sia mediante la localizzazione geografica dei palmari forniti in dotazione agli agenti in servizio.

L'Autorità ha, in primo luogo, ritenuto interamente applicabile la disciplina posta dal Codice, in considerazione della necessaria unicità dell'attività di videosorveglianza svolta in concreto, seppure preordinata alla effettuazione di una pluralità di trattamenti. Tale valutazione è stata effettuata con riguardo ad alcuni specifici trattamenti svolti dal consorzio – in materia di "monitoraggio del traffico" e di "vigilanza sull'integrità e sulla conservazione del patrimonio pubblico e dell'ambiente" non rientranti nell'ambito di applicazione dell'art. 53 del Codice (che dispone una disciplina parzialmente derogatoria in caso di attività svolta da organi di pubblica sicurezza o altri soggetti pubblici per finalità di tutela dell'ordine e della sicurezza pubblica, prevenzione accertamento o repressione dei reati purché prevista da espressa disposizione di legge).

Con riferimento a tale sistema è stata riscontrata l'omessa attivazione della procedura di garanzia prevista dalla disciplina in materia di controlli a distanza sull'attività dei lavoratori (v. artt. 114 del Codice e 4, l. 20.5.1970, n. 300) e la mancata informativa ai diversi soggetti interessati in ordine alle caratteristiche del sistema di videosorveglianza, e – nel dichiarare illecito il trattamento effettuato (e successivamente interrotto) – l'Autorità ha ritenuto che il consorzio, in caso di riattivazione del sistema, dovrà non solo rendere un'idonea informativa ai dipendenti ma anche individuare specifiche modalità per rendere nota alla cittadinanza l'attivazione di tale particolare modalità di sorveglianza (ad es., apponendo idonea cartellonistica e

inserendo informazioni in proposito all'interno dei siti istituzionali dei comuni interessati e del consorzio).

Per quanto riguarda la specifica funzionalità di localizzazione geografica applicata ai dispositivi mobili (palmari) consegnati ai dipendenti, è stato disposto il divieto del trattamento (ancora in atto) sia per l'omessa notificazione al Garante (dovuta ai sensi dell'art. 37 del Codice), sia – anche in questo caso – per la mancata attivazione della procedura di garanzia in materia di controlli a distanza, sia – infine – in considerazione di alcune concrete modalità del trattamento effettuato ritenute eccedenti rispetto alle finalità perseguite (provv. 8 gennaio 2015, n. 2, doc. web n. 3723437).

12.2. *I controlli sull'utilizzo di posta elettronica aziendale e di internet*

Internet

L'utilizzo dei sistemi di comunicazione elettronica (ad es., la posta elettronica aziendale) e internet, – già oggetto, in termini generali, del provv. 1° marzo 2007, n. 13, Linee guida per posta elettronica e internet, doc. web n. 1387522 –, è stato esaminato, in particolare con riguardo al trattamento dei dati personali riferiti alla navigazione internet dei dipendenti, a seguito di accertamenti ispettivi effettuati presso una società operante nel settore dei servizi di comunicazione e promozione commerciale. All'esito dell'accertamento l'Autorità ha dichiarato illecito il trattamento effettuato in violazione degli artt. 11, comma 1, lett. *a*), 13, 114 del Codice, nonché dell'art. 4, l. n. 300/1970, nel testo originario, con la conseguente inutilizzabilità dei dati trattati in violazione di legge, ai sensi dell'art. 11, comma 2, del Codice e disposto il divieto dell'ulteriore trattamento su base individuale dei dati personali riferiti alla navigazione internet dei dipendenti, con conservazione di quelli comunque trattati ai fini della eventuale acquisizione da parte dell'autorità giudiziaria (5 febbraio 2015, n. 65, doc. web n. 3813428).

Oltre, infatti, all'assenza di un'informativa completa circa le effettive caratteristiche del sistema, nonché di una *policy* volta a disciplinare in modo puntuale l'utilizzo degli strumenti elettronici affidati in dotazione ai lavoratori, il sistema era stato configurato con funzionalità tali da permettere la memorizzazione sistematica dell'indirizzo di dettaglio delle singole pagine web (cd. url) richieste e visitate dagli utenti (dipendenti e collaboratori della società), consentendo un controllo della navigazione web individualmente effettuata da soggetti identificabili. Il sistema consentiva, ad es., di generare *report* su base individuale per il tramite dell'amministratore di sistema e di estrapolare i dati di dettaglio relativi alla risorsa internet visitata (url), all'IP sorgente e all'orario di connessione, in presenza di un collegamento univoco tra i dati relativi alla connessione e la persona utilizzatrice, consentendo, quindi, di ricostruirne l'attività (cfr., par. 4 Linee guida cit.; nonché, provv. 21 luglio 2011, n. 308, doc. web n. 1829641, confermata da Trib. Roma, sez. I, 21 marzo 2013 n. 4766; cfr. anche provv.ti 2 aprile 2009, doc. web n. 1606053 e 1° aprile 2010 doc. web n. 1717799).

Trattamenti effettuati sull'*account* di posta elettronica di *ex* dipendenti

Nel solco di un orientamento già espresso con le citate Linee guida per posta elettronica e internet, l'Autorità ha ribadito che il datore di lavoro, in occasione della effettuazione di controlli sul corretto utilizzo di strumenti forniti in dotazione ai dipendenti nell'ambito del rapporto di lavoro, deve in ogni caso salvaguardare la libertà e la dignità dei lavoratori. Inoltre, conformemente ai principi di liceità e correttezza, deve fornire un'informativa chiara e dettagliata in ordine alle consentite modalità di utilizzo degli strumenti aziendali e l'indicazione puntuale delle tipologie di eventuali controlli che possono essere effettuati anche su base individuale. È

stato, pertanto, ritenuto illecito, e conseguentemente vietato, il trattamento effettuato da una società mediante la raccolta e la successiva produzione in giudizio di alcune *e-mail* (con indicazione sia dei dati cd. esterni che del loro contenuto) scambiate tra determinati dipendenti e tra questi e terze persone, senza aver previamente adottato un disciplinare o strumento analogo sull'utilizzo della posta elettronica aziendale e senza aver fornito una specifica informativa ai dipendenti. Il Garante ha, altresì, ritenuto che la società, nel trattare per finalità ulteriori – effettuazione di controlli per dichiarati scopi di tutela del patrimonio aziendale – dati raccolti al diverso fine di consentire la continuità e l'efficienza dei sistemi aziendali, abbia violato il principio di finalità dei trattamenti effettuati (v. art. 11, comma 1, lett. *b*), del Codice).

In conformità ai princìpi in materia di protezione dei dati personali, in caso di cessazione del rapporto di lavoro gli *account* riconducibili a persone identificate o identificabili devono essere disattivati, adottando contestualmente sistemi automatici volti ad informare i terzi ed a fornire a questi ultimi indirizzi alternativi riferiti all'attività professionale del titolare del trattamento. Non è invece conforme ai suesposti princìpi reindirizzare automaticamente su indirizzi di posta elettronica aziendale i messaggi in transito su *account* attribuiti ad *ex* dipendenti (provv. 30 luglio 2015, n. 456, doc. web n. 4298277).

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

La comunicazione e la diffusione dei dati personali riferiti ai dipendenti

L'Autorità continua a ricevere segnalazioni e reclami relativi a forme di conoscibilità di informazioni personali riferite al personale oppure alle modalità di circolazione delle stesse all'interno delle amministrazioni. In particolare, oggetto di verifica sono state le comunicazioni, tramite inoltro di una *e-mail* al personale docente e non docente di un Ateneo, nonché la successiva diffusione, tramite pubblicazione sul sito istituzionale dell'Università, di un documento che conteneva dati personali riguardanti emolumenti erogati in favore di alcuni dipendenti nominativamente indicati; il documento dava conto di presunte irregolarità nella gestione delle risorse economiche. Premesso che il datore di lavoro pubblico può trattare i dati personali dei lavoratori nei limiti in cui ciò sia necessario per la corretta gestione del rapporto di lavoro (cfr. le indicazioni già fornite in via generale con le Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico, adottate con provv. del 14 giugno 2007, n. 161, doc. web n. 1417809), il Garante ha ritenuto, sulla scorta di precedenti in materia che – impregiudicati i profili in ordine alla regolarità sul piano contabile delle erogazioni effettuate –, il personale destinatario della comunicazione elettronica non aveva titolo alcuno per venire a conoscenza dei dati in questione relativi ai colleghi (artt. 3 e 11, comma 1, lett. *d*), del Codice). Sarebbe stato quindi rispettoso del diritto alla dignità, riservatezza e alla protezione dei dati di ciascuno degli interessati provvedere a comunicazioni individualizzate. È stato pertanto dichiarato illecito il trattamento dei dati personali per effetto delle modalità comunicative utilizzate (inoltro a tutto il personale dell'Ateneo di una *e-mail* recante in allegato il cit. documento) per violazione degli artt. 11, comma 1, lett. *a*) e 19, comma 3, del Codice, vietandone l'ulteriore eventuale comunicazione (cfr. già provv. 2 marzo 2011, n. 89, doc. web n. 1802433 e, sul punto, provv. 20 dicembre 2012, n. 431, doc. web n. 2288474 e provv. 18 luglio 2013, n. 358, doc. web n. 2578201, che, con riguardo a specifici casi, hanno confermato le cit. Linee guida, in particolare, punto 5.2). Con la stessa decisione è stata altresì dichiarata illecita la diffusione di dati personali,

contenuti nel medesimo documento, in quanto effettuata in assenza di idonea base normativa (artt. 11, comma 1, lett. *a*) e 19, comma 3, del Codice) ed è stato vietato al titolare del trattamento l'ulteriore diffusione in internet, tramite il sito web istituzionale, dei dati personali riferiti al personale. La pubblicazione del documento all'interno della sezione amministrazione trasparente del siro web dell'Ateneo, infatti, è stata ritenuta illecita, stante la mancata previsione dell'obbligo di pubblicazione di tale tipologia di dati personali tra quelle puntualmente disciplinate dal legislatore nell'ambito del quadro normativo in materia di trasparenza (in particolare, il d.lgs. 14 marzo 2013, n. 33), né, pertanto è stato ritenuto applicabile, come invece sostenuto dall'Universirà, il regime di conoscibilità stabilito dalla normativa sulla trasparenza e in particolare la previsione concernente l'arco remporale quinquennale di permanenza sul web (di cui all'art. 8, comma 3, d.lgs. n. 33/2013; sul punto, cfr. introduzione, parte I, punto I e parte II, provvedimento generale n. 243, 15 maggio 2014, doc. web n. 3134436, Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effertuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati) (provv. 30 luglio 2015, n. 457, doc. web n. 4278610).

12.4. *La pubblicità e trasparenza dei dati dei lavoratori*

In più occasioni il Garante è stato chiamato a pronunciarsi sulla pubblicazione *online* sui siti istituzionali degli enti pubblici ovvero nell'ambito delle sezioni dedicate all'albo pretorio, di dari, atti o provvedimenti contenenti dati personali riferiti a lavoratori - già oggetto di precedenti pronunce e da ultimo con le citate Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicirà e trasparenza sul web da soggetti pubblici e da altri enti obbligati - accertando in molti casi l'illiceità del trattamento per violazione della disciplina di settore (ad es., con riguardo alla mancata osservanza dei termini massimi di pubblicazione) ovvero per mancata osservanza del principio di pertinenza e non eccedenza dei dati pubblicati rispetto alle spesso invocate finalità di adempimento agli obblighi dettati in materia di pubblicità e trasparenza degli atti amministrativi.

In parricolare, a fronte della lamentata pubblicazione di una delibera sul sito web di una Regione, che conteneva valutazioni sulla professionalità e sul contegno di un dipendente e con la quale si disponeva il trasferimento ad altro ufficio, è stata riscontrata l'illiceità della diffusione di tale atto in assenza di idonea base normativa, non potendo a tal fine essere invocata la specifica previsione concernente l'arco temporale quinquennale di permanenza sul web stabilito dalla disciplina in materia di ttasparenza (art. 8, comma 3, d.lgs. n. 33/2013), stante la mancata previsione dell'obbligo di pubblicazione di tale tipologia di atti tra le ipotesi puntualmenre elencate dal legislatore nel capo II del citato decreto o in altra specifica norma in materia di trasparenza. Queste norme – ha ricordato il Garante – prevedono obblighi di pubblicazione nella apposita sezione del sito istituzionale denominata "Amministrazione trasparente" di informazioni "concernenti l'organizzazione e l'attività delle pubbliche amministrazioni" per favorire forme diffuse di controllo sul perseguimento delle funzioni e sull'utilizzo delle risorse pubbliche (artt. 1, comma 1 e 2, comma 2, d.lgs. n. 33/2013) e vanno mantenute distinte, anche sotto il profilo del diverso regime giuridico applicabile, dalle specifiche disposizioni di settore che regolano altri obblighi di pubblicità degli atti amministrativi per finalità diverse dalla trasparenza (cfr. introduzione, parte I, punto I e parte II, Linee guida cit.). Nel

ricordare che l'adempimento ad un obbligo di pubblicazione *online* di informazioni e documenti contenenti dati personali deve avvenire in ogni caso nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato (art. 2 del Codice), l'illiceità della diffusione è stata altresì rilevata anche alla luce del principio di pertinenza e non eccedenza (art. 11, comma 1, lett. *d*), del Codice), atteso che la delibera riportava le valutazioni in merito all'operato del dipendente nell'esecuzione della propria prestazione lavorativa e le specifiche ragioni poste a fondamento del trasferimento ad altro ufficio (provv. 26 marzo 2015, n. 182, doc. web n. 3882453).

12.5. *La pubblicazione* online *di dati idonei a rivelare la condizione di disabilità*

Il Garante è stato nuovamente chiamato a pronunciarsi sulla pubblicazione da parte di soggetti pubblici di graduatorie concorsuali o altri atti immediatamente visibili in rete tramite i più diffusi motori di ricerca generalisti e contenenti in chiaro i dati identificativi riferiti a centinaia di soggetti in condizione di invalidità o disabilità (provv. 24 settembre 2015, n. 489, doc. web n. 4281191). In questo ambito, al fine di sensibilizzare regioni ed enti locali al rispetto della disciplina in materia di protezione dei dati personali, il Presidente dell'Autorità ha inviato due note, indirizzate rispettivamente al Presidente della Conferenza delle regioni e delle province autonome e al Presidente dell'Unione delle province italiane (note 25 settembre, doc. web n. 4281218 e 26 novembre 2015), anche a seguito di alcuni interventi che hanno portato il Garante a dichiarare l'illiceità della diffusione di dati sulla salute dei soggetti interessati (art. 22, comma 8, del Codice) – sovente unitamente ad altre informazioni eccedenti (ad es., in un caso, il codice fiscale degli stessi) – e a disporre il divieto dell'ulteriore diffusione in internet, con la prescrizione ai titolari del trattamento (enti pubblici, aziende sanitarie locali, province e regioni) dell'adozione di idonei accorgimenti nelle operazioni di trattamento funzionali alla pubblicazione di tali atti e attivazione dei conseguenti procedimenti sanzionatori sul piano amministrativo (cfr., anche, le cit. 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, parte II, punti 1 e 3.*b*).

12.6. *I quesiti in materia di trasparenza*

Nel fornire riscontro a specifiche richieste di parere o quesiti formulati dalle pp.aa. e altri soggetti istituzionali, con riguardo all'applicazione della normativa in materia di protezione dei dati nell'ambito dell'osservanza degli obblighi di pubblicazione obbligatoria stabiliti dalla normativa in materia di trasparenza, il Garante ha esaminato una richiesta avente ad oggetto la compatibilità con il quadro giuridico in materia di protezione dei dati personali di una proposta emendativa di norme regolamentari di un Comune. Al fine di dare effettività alle norme in materia di anticorruzione, l'ente locale richiedente intendeva introdurre con proprio regolamento un obbligo di pubblicazione sul web di dati patrimoniali dei dirigenti con incarico a tempo determinato, dei consulenti e collaboratori. Nel prendere atto che il legislatore delegato, nell'esercizio della propria competenza legislativa esclusiva (art. 117, comma 2, lett. *m*), Cost. e art. 1, comma 3, d.lgs. n. 33/2013), ha delimitato le categorie dei soggetti con riguardo ai quali devono essere pubblicate *online* le informazioni relative allo stato patrimoniale degli interessati, il Garante ha preci-

sato che l'eventuale estensione al personale dirigenziale con regolamento comunale degli obblighi di cui all'art. 14, d.lgs. 14 marzo 2013, n. 33 si porrebbe in contrasto con il quadro normativo in materia di protezione dei dati non potendo tale norma - che disciplina, in particolare, gli obblighi di pubblicazione dei dati reddituali e patrimoniali dei soli componenti degli organi di indirizzo politico e dei loro familiari - costituire idonea base normativa per la lecita diffusione delle stesse informazioni riferite anche alla dirigenza pubblica (artt. 4, comma 1, lett. *m*), 11, comma 1, lett. *a*) e 19, comma 3, del Codice). Ai titolari di incarichi dirigenziali e di collaborazione e consulenza trova invece applicazione l'art. 15, d.lgs. n. 33/2013 che prevede la pubblicazione obbligatoria del compenso complessivo percepito dai singoli soggetti interessati, non invece, come detto, la pubblicazione di informazioni relative alle dichiarazioni dei redditi di costoro e dei loro familiari, ipotesi questa che la legge impone esclusivamente nei confronti dei componenti degli organi di indirizzo politico (cfr., punti 9.b. e 9.c, parte I, Linee guida, cit.). Nel sollecitare un bilanciamento fra i valori costituzionali in gioco e il rispetto della normativa comunitaria in materia di protezione dei dati personali sia in fase interpretativa del diritto vigente che in sede di esercizio del potere normativo (cfr. art. 6, par. 1, letr. *c*), e art. 7, par.1, lett. *c*) e *d*), direttiva 95/46/CE; artt. 3 e 11 del Codice; v. inoltre, CGUE, 20/5/2003, cause riunite C-465/00, C-138/01 e C-139/01), il Garante ha ribadito che, più in generale, gli enti locali e le pp.aa. non possono introdurre nuovi obblighi di pubblicazione per finalità di trasparenza con propri atti regolamentari rispetto a quanto già disciplinato dal legislatore, circostanza che potrebbe comportare un'irragionevole differenziazione non solo del livello di trasparenza ma anche, per l'effetto, di quello di protezione dei dari personali sul territorio nazionale a seconda dell'area geografica su cui insistono le competenze istituzionali dell'amministrazione presso cui opera l'interessato ovvero in base al criterio di residenza del cittadino-utente (cfr. già, parere del Garante su uno schema di decreto legislativo concernente il riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pp.aa. del 7 febbraio 2013, n. 49, doc. web n. 2243168) (provv. 25 giugno 2015, n. 377, doc. web n. 4166711).

Con altro quesito è stato richiesto al Garante di formulare un proprio avviso con riguardo alla legittimità della pubblicazione, nella sezione Amministrazione trasparente di un Consiglio regionale, dei nominativi del personale con contratto a tempo determinato in servizio presso le segreterie di supporto ai gruppi politici con indicazione espressa del relativo gruppo di assegnazione. Nel premettere che l'informazione in ordine al gruppo politico in favore del quale si presta collaborazione può, in alcuni casi, rivelare le "opinioni politiche" e, in determinate circostanze, essere indicativo dell'eventuale "adesione a partiti [...o ad] associazioni [...] a carattere [...] politico" (art. 4, comma 1, lett. *d*) ed *m*), del Codice), il Garante ha precisato che in base al quadro di garanzie particolarmente stringente a tutela dei dati sensibili, i soggetti pubblici possono diffondere tali informazioni solo nel caso in cui sia previsto da una espressa disposizione di legge e, pur in presenza di puntuali obblighi di pubblicazione, solo nel caso in cui la diffusione di tali informazioni sia in concreto indispensabile in vista della finalità di rilevante interesse pubblico perseguita (artt. 11, comma 1, lett. *a*) e *d*), 20, 21 e 22, commi 3 e 11, del Codice, ma cfr. anche, art. 4, comma 4, d.lgs. n. 33/2013). Alla luce del quadro normativo (con particolare riferimento agli artt. 16 e 17, d.lgs. n. 33/2013 che mirano a dare evidenza della "dotazione organica" e del "costo del personale"), solo per il personale di diretta collaborazione con gli organi di indirizzo politico che sia, in pari tempo, titolare di un contratto a tempo determinato è prevista la pubblicazione di uno specifico "dato personale" (secondo la definizione del Codice art. 4, comma 1, lett. *b*),

del Codice), quale è il nominativo. Il Garante ha, quindi, concluso che la Regione poteva disporre la pubblicazione nella sezione Amministrazione trasparente del sito web del Consiglio regionale dei soli dati personali espressamente previsti dalla legge, ossia i nominativi del personale a tempo determinato, senza specificare, per coloro che svolgano servizio presso le segreterie di supporto ai gruppi politici, il relativo gruppo politico di assegnazione (v. art. 1, comma 2, nonché, artt. 4, 6, 8 comma 3, d.lgs. n. 33/2013; art. 8, par. 1, direttiva 95/46/CE, nonché WP Art. 29, *Advice paper on special categories of data (sensitive data)*, 4 aprile 2011) (provv. 25 giugno 2015, n. 376, doc. web n. 4699444).

12.7. *La comunicazione tra soggetti pubblici di dati relativi ai lavoratori*

Il Garante si è altresì pronunciato con riguardo alle istanze formulate ai sensi degli artt. 19, comma 2, e 39 del Codice. In particolare, il Comando di polizia locale di un Comune aveva rappresentato la necessità di ottenere l'autorizzazione a comunicare alla Regione di competenza alcuni dati personali riferiti agli operatori di polizia locale al fine di consentire la realizzazione di tessere di riconoscimento per il personale di polizia locale operante nel tetritorio tegionale. Tanto, in base al quadro normativo di riferimento e in attuazione di un apposito accordo tra la Regione stessa ed i Comuni interessati. Il Garante ha ritenuto che la fornitura di tessere di riconoscimento per il personale di polizia locale potesse essere inquadrata nell'ambito delle funzioni istituzionali di coordinamento, sostegno e supporto tecnico e finanziario in favore degli enti locali e dovesse essere considerata nell'ambito della tealizzazione di progetti per la sicurezza urbana, nonché di sostegno all'attività operativa della polizia locale; ciò, sia con riguardo alla disciplina quadro in materia di ordinamento di polizia locale (cfr. art. 6, comma 2, l. 7 marzo 1986, n. 65) che alla vigente disciplina regionale di settore. Considerata la mancanza di un'espressa previsione di legge o di regolamento che in via diretta preveda la comunicazione di dati personali degli addetti al servizio di polizia locale da parte dei Corpi operanti presso i singoli Comuni a favore della Regione, il Garante, ai sensi degli artt. 19, comma 2, e 39, comma 2, del Codice, ha stabilito che i Corpi di polizia locale presso i Comuni interessati, possono lecitamente comunicare alla Regione i pertinenti dati personali (art. 11, comma 1, lett. *d*), del Codice) riferiti al personale addetto al servizio di polizia locale e che la Regione può, a propria volta, anche per il tramite di soggetti designati responsabili del trattamento, procedere allo svolgimento delle attività di trattamento necessarie alla predisposizione e gestione delle tessere di riconoscimento, nel rispetto dei princìpi di necessità pertinenza e non eccedenza, anche sotto il profilo dei tempi di conservazione (artt. 3, 11, comma 1, lett. *b*) ed *e*), del Codice) nonché delle disposizioni che stabiliscono le misure di sicurezza (artt. 31, 33 e 34 del Codice) (provv. 28 maggio 2015, n. 317, doc. web n. 4169391).

13 Le attività economiche

13.1. *Il settore bancario*

Anche nel 2015 sono pervenute numerose segnalazioni e reclami riguardanti problematiche sulle quali il Garante ha già avuto modo di pronunciarsi con le Linee guida adottate il 25 ottobre 2007 in materia di trattamenti di dati personali effettuati da banche nei rapporti con la clientela (doc. web n. 1457247). Le istanze hanno riguardato, in particolare, i profili dell'accesso ai dati relativi a rapporti bancari (in specie di conto corrente e depositi titoli) di persone decedute, quello della richiesta di copia di documentazione riferita a rapporti bancari e quello della comunicazione a terzi di dati inerenti a clienti.

Il flusso costante di segnalazioni in questo ambito appare legato soprattutto all'attuale situazione di profonda crisi economica che, determinando l'aumento delle posizioni bancarie di temporanea difficoltà o di "sofferenza", moltiplica inevitabilmente il contenzioso banche/clientela e aumenta la necessità di ricostruire la "storia" dei rapporti contrattuali, specie con riguardo agli interessi praticati. Negli ultimi mesi, poi, appare evidente l'attenzione di numerosi correntisti degli istituti di credito interessati dalle recenti vicende di ristrutturazione o dissesto, vicende che hanno portato con sé l'esigenza dei risparmiatori di verificare la completezza e la "trasparenza" delle informazioni ricevute dagli istituti di credito.

Circolazione delle informazioni e tracciamento delle operazioni bancarie

Con riferimento ai più volte segnalati casi di illecita comunicazione di dati a terzi non legittimati, è proseguita l'attività di monitoraggio dell'adempimento da parte delle banche alle misure (sia necessarie che opportune) prescritte dal Garante all'intero settore creditizio con il provvedimento generale – adottato il 12 maggio 2011 e divenuto pienamente efficace il 1° ottobre 2014 – recante Prescrizioni in mareria di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie (provv. n. 192, doc. web n. 1813953).

In tale ambito, il Garante ha deliberato di indirizzare parte dell'attività ispettiva di iniziativa curata dall'Ufficio alla verifica dell'implementazione delle prescrizioni contenute nella decisione, al fine di valutare gli effetti prodotti da un provvedimento di sicuro rilievo nella configurazione del rapporto banca/clientela, specie in riferimento alla sentita necessità di innalzare il livello di protezione dei dati personali dei clienti.

Nel corso dell'anno, pertanto, sono state effettuate diverse ispezioni nei confronti di istituti di credito, individuati a campione anche in relazione alle diverse tipologie dimensionali e operative. L'attività ispettiva proseguirà anche nel primo semestre del 2016, con l'obiettivo di fornire agli operatori coinvolti, ove all'esito dei controlli effettuati se ne dovesse ravvisare la necessità, ulteriori indicazioni, anche operative, di carattere generale.

13.2. *La revisione del codice deontologico Sic*

La grande attenzione al tratramento dei dati in ambito bancario e finanziario ha da molti anni spinto l'Autorità a confronrarsi con il correlato tema delle grandi banche dati che, già previste dal legislatore o costituite per iniziativa degli operatori del set-

tore, svolgono la delicata funzione di condividere dati e informazioni sulla situazione economica di persone fisiche e imprese al fine di indirizzare le decisioni sulla concessione del credito, attenuando il relativo rischio. Dalla più antica centrale dei rischi della Banca d'Italia ai sistemi di informazione creditizia gestiti da soggetti privati, sottoposti ad un codice di deontologia varato nell'ormai lontano 2004, sono numerosi gli strumenti di questo tipo quotidianamente consultati dagli operatori del settore. Si tratta di strumenti ormai connaturati al funzionamento del sistema creditizio e inseriti in un panorama nel quale operano anche la centrale d'allarme interbancaria e le società che forniscono servizi di informazione commerciale, realtà che parimenti sono spesso destinatarie di istanze di esercizio dei diritti di cui all'art. 7 del Codice.

In questo quadro economico e normativo, sono proseguiti i lavori volti alla revisione del cd. codice deontologico Sic, a dieci anni dalla sua entrata in vigore.

L'Autorità ha ultimato la verifica dei requisiti di partecipazione al tavolo di lavoro prescritti dal provvedimento 17 aprile 2014, n. 203 (doc. web n. 3070048) – nel rispetto del principio di rappresentatività di cui all'art. 2, comma 2, reg. n. 2/2006 del Garante sulle procedure per la sottoscrizione dei codici di deontologia e di buona condotta – in capo ai soggetti interessati a prendervi parte e ha formalizzato l'esclusione di quelli privi dei requisiti richiesti, comunicando, invece, l'avvio dei lavori a quelli ammessi a parteciparvi.

Nel corso di specifici incontri, sono state individuate le tematiche da approfondire in sede di revisione del codice e la metodologia da seguire, costituendo a tal fine un tavolo tecnico ristretto composto, tra gli altri, da rappresentanti dei gestori dei Sic, degli istituti di credito e delle società finanziarie (i cd. partecipanti) e delle associazioni dei consumatori e deputato a proporre le modifiche da apportare al codice e, in generale, ad interagire con l'Autorità per garantire un più agevole e spedito svolgimento dei lavori.

Alcuni dei partecipanti ai lavori hanno sollevato, in via preliminare, il problema del ruolo da attribuire ai nuovi soggetti che "possono avere accesso" ai Sic ai sensi dell'art. 6-*bis*, d.l. 13 agosto 2011, n. 138 (inserito dalla l. di conversione 14 settembre 2011, n. 148, per effetto del rinvio all'art. 30-*ter*, d.lgs. 13 agosto 2010, n. 141), avuto riguardo, in particolare, ai fornitori di servizi di comunicazione elettronica e alle imprese di assicurazione.

La questione sollevata, da definire nel corso del 2016 e propedeutica al prosieguo dei lavori, mira, nelle intenzioni dei proponenti, a prevedere che tali "nuovi" soggetti contribuiscano nei cd. Sic anche i dati relativi ad interessati privi di una storia creditizia, in modo da diventare "partecipanti pieni" (come definiti dall'art. 1, comma 1, lett. *e*) del codice deontologico) ai sistemi di informazioni creditizie conformemente al principio di reciprocità che ha finora presieduto alla costituzione di questo tipo di banche dati.

13.3. *Il fenomeno delle morosità nel settore delle cd.* utilities

Costituzione di una banca dati relativa a morosità intenzionali nel settore telefonico (S.I.Mo.I.Tel.)

Il rilievo e le potenzialità espresse nell'ambito economico-finanziario dalle diverse centrali rischi cui si è fatto cenno nei paragrafi precedenti, hanno innescato da alcuni anni la spinta (prima a livello di riflessione nell'ambito delle categorie economiche e professionali, poi anche a livello di progettazione normativa) a riprodurre questo modello anche in ambiti molto diversi da quelli da cui storicamente ha tratto origine. Poiché, a tutt'oggi, manca un organico quadro normativo (di cui peraltro si avverte sempre di più la necessità), il Garante si è trovato (e si trova) nella necessità di esaminare, sulla base dei princìpi generali del Codice e della normativa comuni-

taria per i profili di interesse, i diversi progetti che al riguardo vengono, con sempre maggiore frequenza, proposti. Da questo punto di vista, l'anno 2015 ha costituito una tappa significativa; primo banco di prova è stato rappresentato dal settore delle telecomunicazioni.

L'8 ottobre 2015, al termine di un intenso confronto che ha accompagnato e seguito la consultazione pubblica relativa allo schema di provvedimento già adottato dall'Autorità con delibera n. 154 del 27 marzo 2014 e relativo al progetto di costituzione del cd. SIT (provv. n. 523, doc. web n. 3041680), è stato adottato un ptovvedimento che prevede la costituzione di una banca dati relativa a morosità intenzionali della clientela del settore telefonico (doc. web n. 4349760). A seguito di numerose riserve sollevate soprattutto dalle associazioni dei consumatori e di profili problematici rappresentati anche dal Consiglio nazionale dei consumatori e degli utenti presso il Ministero dello sviluppo economico, l'Autorità ha svolto numerosi incontri con i rappresentanti degli operatori telefonici e con un'ampia rappresentanza di associazioni di consumatori. L'attività di dialogo e confronto e l'ampio coinvolgimento di realtà associative ha portato all'elaborazione di proposte operative in larga parte condivise tra le parti e poi recepite nel provvedimento. La banca dati di cui si è prevista la costituzione è radicalmente diversa da quella inizialmente ipotizzata, non essendo più assimilabile a una centrale rischi negativa di settore, ma piuttosto ad un sistema che censirà solo coloro (persone fisiche e giuridiche, enti, associazioni, titolari di ditte individuali e liberi professionisti) che non paghino intenzionalmente le bollette telefoniche relative a pacchetti comprensivi di abbonamento e fornitura di *smartphone* o *tablet*, con esclusione, invece, dei soggetti che si rendano eventualmente e temporaneamente inadempienti ai propri obblighi contrattuali perché inesperti, distratti o interessati da momentanee difficoltà economiche. Obiettivo del provvedimento è dunque quello di contrastare il fenomeno del cd. "turismo telefonico", costituito da utenti che passano da un operatore all'altro lasciando intenzionalmente bollette insolute pur avendo acquisito la disponibilità di un dispositivo spesso di significativo valore economico. Da qui l'individuazione della nuova denominazione di Sistema informativo sulle morosità intenzionali nel settore della telefonia (S.I.Mo.I.Tel.), che sottende una profonda differenza dello strumento e delle sue finalità rispetto a quello originariamente ipotizzato.

Lo scambio di informazioni sulle morosità intenzionali tra gli operatori telefonici (partecipanti alla banca dati) può quindi risultare uno strumento utile per valutare e contenere condotte destinate ad incidere non solo sui bilanci degli operatori, ma anche su altri utenti incolpevoli e in regola con i pagamenti, i quali potrebbero essere costretti a sopportare costi altrimenti non dovuti. Nel Sistema – consultabile dagli operatori prima dell'attivazione di un nuovo contratto e gestito da un soggetto che verrà individuato dagli stessi operatori telefonici, presumibilmente entro l'anno 2016 – potranno essere trattate solo informazioni riguardanti i mancati pagamenti del cliente ad esclusione, in particolare, di dati sensibili e giudiziari. Le informazioni sulle morosità potranno essere inserite nel S.I.Mo.I.Tel. solo in presenza di specifici requisiti: recesso dal contratto da non meno di tre mesi; morosità superiore a 150 euro per singolo operatore; fatture non pagate nei primi sei mesi successivi alla stipula del contratto; assenza di altri contratti tutt'ora attivi con lo stesso operatore. Prima di essere inserito nel sistema il cliente dovrà essere avvertito dall'operatore telefonico dell'imminente iscrizione. Le informazioni sui pagamenti non regolarizzati saranno conservate per 36 mesi e poi verranno cancellate automaticamente. I dati raccolti non potranno essere usati per altre finalità (ricerche di mercato, pubblicità, *marketing*). In applicazione dell'istituto del bilanciamento di interessi, previsto dall'art. 24, d.lgs. n. 196/2003, l'Autorità ha ritenuto che il trattamento dei

dati contenuti nel S.I.Mo.I.Tel. possa essere effettuato dal gestore del Sistema e dagli operatori telefonici senza consenso degli interessati, purché sia preceduto da un'informativa chiara e puntuale da rendere in occasione della stipula del contratto. Allo scopo di gestire la fase di avvio del sistema, si è anche previsto che, entro 60 giorni dalla pubblicazione del provvedimento in Gazzetta Ufficiale, gli operatori rendano anche un'informativa preventiva all'ampia platea di clienti i cui rapporti sono già in essere e che potrebbero essere censiti nella banca dati. Una volta che gli operatori telefonici avranno individuato il soggetto privato cui affidare la gestione del Sistema, dovranno comunicare al Garante il nome e la sede della banca dati, ed almeno tre mesi prima dell'entrata in funzione, dovranno inviare copia dell'accordo sottoscritto dalle parti per consentire all'Autorità di valutarne la conformità alle prescrizioni dettate. Al gestore spetta invece l'obbligo di notificare al Garante il trattamento dei dati prima del suo inizio.

La collaborazione con l'Autorità per l'energia elettrica e il gas

L'Autorità ha reso all'Autorità per l'energia elettrica ed il gas la richiesta collaborazione per valutare la correttezza del trattamento dei dati personali della clientela derivante da specifici interventi ipotizzati da Aeeg e volti a contrastare, nel breve periodo, la rilevante crescita del fenomeno della morosità nel mercato di riferimento.

In particolare, sono state fornite talune indicazioni affinché il trattamento da parte del nuovo venditore (di energia elettrica e gas) di dati personali ulteriori (rispetto a quelli contenuti nei contratti) dei clienti interessati alla procedura di cd. *switching* – già puntualmente regolamentata con disposizioni di rango primario e secondario – sia anche conforme al Codice. I chiarimenti resi mirano a consentire una più precisa e completa valutazione delle condizioni in cui avverrà la futura fornitura e permettere, eventualmente, di rinunciare al cambio richiesto revocando il contratto concluso prima della sua esecuzione (nota 8 maggio 2015, doc. web n. 4702076).

13.4. *Il nuovo codice di deontologia e di buona condotta in materia di informazioni commerciali*

L'attenzione al tema delle grandi banche dati ha portato anche alla definizione delle regole di deontologia per il trattamento dati in un settore, quello delle informazioni commerciali, che pur essendo storicamente consolidato, si è mosso per lunghi anni in un ambito estremamente povero di riferimenti normativi. Al termine di un'istruttoria lunga e complessa, durata circa cinque anni, con il provvedimento 17 settembre 2015, n. 479 (doc. web n. 4298343) è stato adottato il codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato ai fini di informazione commerciale (v. art. 118 del Codice) destinato a tutti i soggetti che si trovino o vogliano operare nel settore relativo alle attività di informazione commerciale sul territorio italiano (ai sensi dell'art. 134, r.d. n. 773/1931, e successive modificazioni ed integrazioni, recante il t.u. delle leggi di pubblica sicurezza e relativi regolamenti di attuazione). In particolare, non solo viene sancito che l'attività di raccolta delle informazioni debba avvenire nel rispetto dei diritti, delle libertà fondamentali e della dignità delle persone interessate, e segnatamente del diritto alla protezione dei dati personali, del diritto alla riservatezza e del diritto all'identità personale (art. 2 del Codice), ma vengono, altresì individuate, nel rispetto dei princìpi sanciti dall'art. 11 del Codice, adeguate garanzie e modalità di trattamento dei dati personali che mirino a garantire la qualità, la pertinenza, l'esattezza e l'aggiornamento dei dati personali trattati. Profilo questo di particolare rilievo in quanto, nella corrente attività d'impresa, le decisioni quotidianamente assunte in sede di contrattazione fra diversi sog-

getti economici e ancor più le decisioni in materia di finanziamento vengono assunte proprio sulla base dei *report* informativi e delle valutazioni espresse dagli operatori della cd. informazione commerciale. Naturalmente, il codice deontologico si applica alle sole informazioni commerciali riferite a persone fisiche (rientranti nel concetto di interessato di cui all'art. 4, comma 1, lettera *i*), del Codice) ed, in particolare, al trattamento dei dari personali provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque o pubblicamente accessibili da chiunque, nonché al trattamento avente ad oggetto i dati personali forniti direttamente dagli interessati, effettuato dai soggetti che prestano a terzi servizi, per finalità di informazione commerciale, nel rispetto dei limiti e delle modalità che le normative vigenti stabiliscono per la conoscibilità, utilizzabilità e pubblicità di tali dati; resta, pertanto, esclusa la sua applicazione alle informazioni commerciali riferite alle persone giuridiche. Il codice, infine, detta regole più semplici sia relativamente all'informativa, sia relativamente all'esercizio dei diritti dell'interessato. Particolarmente significativa e oggetto di un'elaborazione attenta e prudente, è la disciplina concernente la possibilità di trattare informazioni tratte da fonti giornalistiche sia cartacee che *online* (di cui all'art. 3, comma 2, del codice di deontologia). È un'apertura verso un modello di informazione commerciale più completo e circostanziato, ma anche più esposto a rischi di inesattezza o comunque suscettibile di costante aggiornamento. Ne è specifica testimonianza anche la disposizione sul trattamento dei dati giudiziari (di cui al comma 5 del cit. art. 3). Non meno rilevante è, poi, il complesso di disposizioni che (specie nell'art. 7) mirano a delimitare il perimetro dei soggetti censibili e soprattutto l'eventuale collegamento degli stessi con le realtà imprenditoriali e societarie nelle quali hanno operato o rispetto alle quali hanno esercitato ruoli o nelle quali sono stati titolari di posizioni volta a volta ritenute significative e rilevanti.

13.5. *Il settore assicurativo*

In ambito assicurativo, l'Autorità è stata più volte chiamata a esprimere il proprio parere in merito ad alcuni atti regolamentari o provvedimentali adottati dall'Ivass. Ciò, con riferimento particolare a quel complesso di banche dati di recente costituzione, implementate essenzialmente per consentire una più efficace attività antifrode nel settore della responsabilità civile automobilistica.

Con riferimento alla banca dati degli attestati di rischio (art. 134, comma 2, d.lgs. n. 209/2005), il Garante, nell'esprimere parere sul regolamento Ivass n. 9 del 19 maggio 2015, sul collegato provvedimento n. 35 del 19 giugno 2015 e sui relativi allegati tecnici (provv. 30 luglio 2015, n. 454, doc. web n. 4252652), ha richiamato l'Istituto sulla necessità di perfezionare i testi sottoposti ad esame, sia per quanto riguarda la specificazione del ruolo delle imprese in fase di alimentazione e consultazione della banca dati, delle finalità sottese alla trasmissione delle informazioni e delle misure di sicurezza da garantire a protezione di queste ultime (regolamento), sia per quel che concerne il richiamo al rispetto della disciplina del Codice e ai diritti degli interessati, il rilascio di alcune opportune indicazioni in tema di informativa e consenso, la previsione di un termine massimo di conservazione delle informazioni. Non sono risultati problematici, invece, altri profili regolarori concernenti, in particolare, la proporzionalità del trattamento e la qualità dei dati.

Su altro versante, il Garante è stato poi chiamato a valutare talune modifiche che l'Ivass avrebbe voluto apportare, sulla base di alcuni interventi normativi anche recenti e delle osservazioni pervenute all'esito della pubblica consultazione, al "nuovo" schema di regolamento recante la disciplina della banca dati sinistri, della banca dati anagrafe

testimoni e della banca dati anagrafe danneggiati (art. 120 del Codice; art. 135, d.lgs. n. 209/2005). L'Autorità ha ricordato, tra l'altro, la necessità di rispettare i principi di finalità e proporzionalità, circoscrivendo l'accesso alle informazioni contenute nelle predette banche di dati ai soli soggetti legittimati in base alla legge, oltre che in rapporto alle finalità "antifrode" sottese alla loro istituzione (art. 11, comma 1, lett. *b*) e *d*), del Codice). Inoltre, è stata chiarita la necessità di modificare il testo nella parte relativa alla nozione di "interessati", non più comprensiva dei soggetti riconducibili a persone giuridiche, enti o associazioni (art. 40, d.l. 6 dicembre 2011, n. 201, convertito con modificazioni dalla l. 22 dicembre 2011, n. 214).

13.6. *La videosorveglianza in ambito privato*

Nel corso dell'anno, è proseguito l'afflusso di segnalazioni e reclami concernenti le più svariate ipotesi di installazione di videocamere. La tipologia di istanze proposte conferma l'elevato livello di contenzioso sia con riguardo alle installazioni per finalità esclusivamente personali (art. 5, comma 3, del Codice) sia con riguardo a quelle in ambito condominiale.

La base di riferimento è ovviamente costituita dal provvedimento generale dell'8 aprile 2010 (doc. web n. 1712680) in ordine al quale l'Ufficio ha avviato un lavoro di revisione e aggiornamento tenendo conto anche delle novità tecnologiche che moltiplicano la possibilità di effettuare videoriprese (basti pensare all'utilizzo di droni o alla diffusione delle cd. *dash cam*).

Per ciò che riguarda, invece, le istanze di verifica preliminare sottoposte al Garante, vale rilevare che tutte hanno riguardato la richiesta di allungare i tempi di conservazione delle immagini registrate dai sistemi di videosorveglianza oltre i sette giorni al fine di rafforzare il livello di sicurezza del sito oggetto di videosorveglianza.

In particolare, si è trattato di aziende che operano nel campo della produzione di beni anche di lusso e dei trasporti intermodali di merci. Tutte le richieste hanno avuto un esito favorevole e sono state valutate tenendo in considerazione, non solamente i parametri di sicurezza previsti dalle normative internazionali, comunitarie e nazionali, ma le acclarate difficoltà delle società di accertare, in tempi più contenuti, eventuali illeciti verificatisi. Ciò in relazione alle tempistiche connesse alla verifica delle giacenze o a quelle relative alle spedizioni internazionali.

13.7. *Il recupero crediti*

È un'attività che dà luogo ad un trattamento dati spesso molto invasivo e, per le concrete modalità del suo svolgersi, difficilmente monitorabile, rispetto al quale, quindi, è più difficile individuare comportamenti illeciti. Con riferimento ad un trattamento "tracciabile" il Garante, con provvedimento del 28 maggio 2015, n. 319 (doc. web n. 4131145), a seguito della segnalazione di un abbonato di Sky Italia s.r.l., si è pronunciato su un sistema che la società aveva predisposto per recuperare importi insoluti dovuti dai propri clienti. Il sistema prevedeva l'invio, al *decoder* del cliente, di messaggi di sollecito visualizzabili sullo schermo del televisore sotto forma di *banner* contenenti l'icona di una busta: il tasto del telecomando che consentiva la lettura del messaggio, oppure la chiusura del *banner* per leggere il messaggio in un secondo momento, poteva essere azionato senza limitazioni da chiunque si trovasse davanti allo schermo; ne conseguiva la possibilità che terzi estranei conoscessero la posizione debitoria dell'abbonato (peraltro contestata in concreto dal segnalante). Il Garante,

richiamando anche le ptescrizioni già rese in passato in materia di trattamenti di dati personali effettuati nell'esercizio di attività di recupero in sede stragiudiziale di crediti (v. provv. generale 30 novembre 2005, doc. web n. 1213644), ha stabilito che tale trattamento di dati non fosse lecito, tenuto conto che, per le modalità utilizzate, lo stato di insolvenza degli abbonati si prestava ad essere conosciuto da un numero indeterminato di soggetti; ha pertanto prescritto a Sky Italia s.r.l., qualora inrendesse continuare ad utilizzare il sistema dei messaggi sul televisore anche per finalità di recupero crediti, di adottare specifiche misure volte ad escludere il rischio, anche potenziale, di diffusione a terzi di informazioni sulla situazione debitoria dei propri abbonati. In particolare la società avrebbe dovuto prevedere l'utilizzo di un codice di accesso al contenuto del messaggio da consegnare a qualunque cliente al momento della sottosctizione del contratto e da utilizzare per leggere il messaggio, ferma restando la necessità di privilegiare, in ogni caso, per l'invio di solleciti di pagamento altre modalità, quali ad esempio la comunicazione via *e-mail* o l'invio di una comunicazione all'indirizzo del cliente. La società ha successivamente comunicato al Garante di essersi adeguata alle prescrizioni contenute nel provvedimento e di averne dato notizia alla clientela con apposito comunicato stampa.

13.8. *Altre attività imprenditoriali*

Autonoleggio ed *event data recorder*

Come nel 2013 (v. provv. 7 novembre 2013, n. 499, doc. web n. 2911484), l'Autorità è stata chiamata a valutare la liceità dei trattamenti connessi all'installazione, a bordo del parco veicoli in dotazione a una società di autonoleggio, di dispositivi satellitari multifunzione annoverabili tra i cd. *event data recorder*. Tali dispositivi, in grado di raccogliere e trasmettere ad appositi fornitori di servizi numerose informazioni relative alle singole vetture (e indirettamente, ai relativi conducenti), sarebbero stati utilizzati dalla società per garantire alcuni servizi (gestione di eventuali sinistri; ritrovamento dei veicoli rubati; assistenza stradale; monitoraggio chilometri e tempi di utilizzo; diagnostica) ai propri clienti. All'esito di una complessa attività istruttoria, l'Autorità ha ammesso i trattamenti oggetto dell'istanza, ritenendoli conformi – ove effettuati nel rispetto delle modalità indicate – ai princìpi di liceità, necessità, finalità e proporzionalità (artt. 3 e 11 del Codice); tuttavia, sono state prescritte alla società alcune misure volte ad assicurare un'effettiva tutela degli interessati, sia sul piano delle misure di sicurezza e dei requisiti che devono possedere, rispettivamente, i fornitori dei servizi descritti e i dispositivi eletttonici utilizzati (ove carenti in tal senso), oltre che il portale web accessibile dal titolare, sia sul piano della modulistica utilizzata ai fini del rilascio dell'informativa agli interessati e dell'acquisizione del relativo consenso (da emendare in funzione delle indicazioni contenute nel provvedimento adottato). Nel prescrivere, tra le altre, anche la distruzione dei dati personali non più necessari in rapporto agli scopi petseguiti nell'ambito dei singoli servizi offerti, ha poi ribadito che i dati trattati attraverso tali tipologie di sistemi non possono essere utilizzati dai titolari per finalità diverse da quelle dichiarate e, in particolare, per profilare i conducenti o negare la stipula di nuovi contratti di autonoleggio (provv. 7 maggio 2015, n. 270, doc. web n. 4167756).

Franchising

A seguito di un reclamo, l'Autorità è stata poi chiamata a valutare la liceità del trattamento effettuato da alcuni collaboratori operanti nell'interesse, tra l'altro, di un *franchisor*. La reclamante contestava l'invio (documentato in atti), da parte dei predetti collaboratori, di una *e-mail* contenente propri dati personali e sensibili ad alcuni *franchisee*, senza che tale comunicazione fosse sorretta da adeguati presupposti giustificativi. A seguito di una approfondita istruttoria – volta a chiarire, in capo