Più in generale, nel periodo di riferimento sono state anche effettuate:

- verifiche sull'adozione delle misure minime di sicurezza da parte di soggetti, pubblici e privati, che effettuano trattamenti di dati sensibili;
- altre verifiche di iniziativa concernenti, in particolare, l'adempimento dell'obbligo di notificazione da parte di soggetti, pubblici e privati, individuati mediante raffronto con il registro generale dei trattamenti;
- verifiche con particolare riferimento al rispetto dell'obbligo di informativa, alla pertinenza e non eccedenza nel trattamento, alla libertà e validità del consenso, nonché alla durata della conservazione dei dati nei confronti di soggetti, pubblici o privati, appartenenti a categorie omogenee. Ciò, prestando anche specifica attenzione a profili sostanziali del trattamento che spiegano significativi effetti sulle persone da esso interessate.

### 17.2. LA COLLABORAZIONE CON LA GUARDIA DI FINANZA

Anche nell'anno di riferimento l'Autorità si è avvalsa della preziosa collaborazione della Guardia di finanza per lo svolgimento dell'attività di controllo, in applicazione del protocollo di intesa siglato nel 2005. Al riguardo si fa rinvio a quanto nel dettaglio riferito nelle precedenti Relazioni (cfr., da ultimo, Relazione 2009, p. 240 ss.), evidenziando ancora una volta la meritoria attività svolta dal Nucleo speciale *privacy*, che ha direttamente effettuato la gran parte degli accertamenti delegati, avvalendosi anche, ove necessario, dei reparti del Corpo territorialmente competenti.

Sulla base della prassi operativa ormai consolidata, le informazioni e i documenti acquisiti nell'ambito degli accertamenti dal Corpo, sono trasmessi all'Autorità per le successive verifiche in ordine alla liceità del trattamento e al rispetto dei princìpi previsti dalla legge.

Laddove emergano violazioni penali o amministrative, la Guardia di finanza provvede direttamente a informare l'autorità giudiziaria competente e a formalizzare la contestazione delle sanzioni amministrative accertate.

In tal modo l'Autorità dispone di un dispositivo di controllo flessibile ed articolato che integra l'attività svolta direttamente dal dipartimento ispettivo dell'Autorità e che consente tempestive ed efficaci verifiche sul territorio.

Particolare attenzione è stata rivolta alla formazione del personale incaricato dell'attività ispettiva.

Oltre agli ordinari corsi presso la Scuola di polizia tributaria, denominati "Collaborazione della Guardia di finanza con l'Autorità Garante per la protezione dei dati personali", diretti a illustrare al personale operante nei reparti territoriali del Corpo i princìpi del Codice e le prassi operative nei controlli in materia di *privacy*, è stato anche realizzato un innovativo corso per il personale del Nucleo addetto alle ispezioni e i funzionari dell'Autorità, denominato "*Data Protection Enforcement* - attività di controllo delle banche dati".

Tale attività formativa si colloca nell'ambito delle azioni di accrescimento dell'efficacia dei controlli effettuati sia dal personale del Garante sia da quello della Guardia di finanza, anche sulla scorta di quanto previsto dal protocollo d'intesa tra la Guardia di finanza e l'Autorità.

In tale contesto si è sentita l'esigenza di accrescere le conoscenze di natura tecnico-informatica, per acquisire metodologie utili per l'effettuazione degli accessi alle banche dati, così da individuare in modo più accurato eventuali violazioni.

L'iniziativa, preceduta da un'articolata fase di progettazione, si è sviluppata su tre distinti moduli, il primo dei quali curato dal Servizio informatica del Comando generale della Guardia di finanza, il secondo affidato ad una società di formazione specializzata nel settore e l'ultimo, di natura teorico-pratica, curato da personale dell'Ufficio in possesso di peculiari competenze.

L'attività, che ha riguardato complessivamente 32 persone (di cui 24 militari del Nucleo speciale *privacy* e 8 funzionari dell'Autorità), ha avuto un riscontro ampiamente positivo da parte di tutti i frequentatori e ha comportato un significativo miglioramento della qualità e delle modalità di redazione delle risultanze documentali, che consentirà una migliore valutazione dei fenomeni oggetto delle attività istruttorie.

### 17.3. I SETTORI OGGETTO DEI CONTROLLI E I CASI PIÙ RILEVANTI

Nel 2011 le ispezioni hanno riguardato:

- 50 controlli nei confronti di ospedali pubblici e cliniche private, con riferimento alla liceità dei trattamenti effettuati e all'adozione delle misure minime di sicurezza;

- 40 controlli nei confronti di fornitori di energia elettrica e gas, con riferimento all'utilizzo dei dati dei clienti;
- 40 controlli nei confronti di società che organizzano eventi e gestiscono parchi giochi, con riferimento al trattamento dei dati dei clienti e all'utilizzo di sistemi di videosorveglianza;
- 40 controlli nei confronti di investigatori privati, con riferimento al rispetto del Codice di deontologia e di buona condotta per i trattamenti di dati personali effettuati per svolgere investigazioni difensive;
- 30 controlli nei confronti di società che forniscono beni e servizi via internet (*e-commerce*), con riferimento all'utilizzo dei dati dei clienti, anche per finalità di *marketing*;
- 22 controlli nei confronti di società che effettuano l'attivazione di schede telefoniche (*dealer*) per conto di società telefoniche, con riferimento alla liceità dell'utilizzo dei dati dei clienti per l'intestazione delle schede stesse;
- 20 controlli nei confronti di società che gestiscono scuole per il rilascio di patenti nautiche, con riferimento all'utilizzo dei dati dei clienti;
- 15 controlli nei confronti di centri per l'impiego, con riferimento all'utilizzo dei dati delle persone che usufruiscono dei loro servizi, con particolare riferimento all'adozione delle misure di sicurezza;
- 9 controlli nei confronti di società che commercializzano via internet coupon per l'acquisto di beni e servizi offerti da terzi, con riferimento all'acquisizione del consenso degli interessati e all'utilizzo dei dati dei clienti per finalità di *marketing*;
- 8 controlli nei confronti di società che commercializzano banche dati per finalità di *marketing* effettuato anche attraverso l'invio di sms, mms ed e-mail, volti a verificare la liceità del trattamento, con particolare riferimento al consenso degli interessati all'utilizzo dei propri dati;
- 6 controlli nei confronti di grandi catene alberghiere, autonoleggi e *tour operator* relativamente alle modalità di utilizzo dei pagamenti dei clienti attraverso carte di credito;
- 5 controlli nei confronti di società e/o enti che utilizzano sistemi di localizzazione satellitare, per verificare il rispetto del provvedimento generale adottato in materia dal Garante (provv. 4 ottobre 2011 [doc. *web* n. 1850581]);

- 5 controlli nei confronti di società telefoniche, con riferimento alla profilazione dei clienti per verificare il rispetto delle misure e accorgimenti prescritti dal Garante in sede di verifica preliminare, nonché il rispetto del provvedimento generale "Prescrizioni ai fornitori di servizi di comunicazione elettronica accessibili al pubblico che svolgono attività di profilazione" (provv. 5 giugno 2009 [doc. *web* n. 1629107]);
- 4 controlli nei confronti di società di riscossione crediti, con riferimento alla liceità della raccolta dei dati dei soggetti nei cui riguardi svolgono la propria attività;
- 3 società che gestiscono giochi e scommesse, con riferimento all'utilizzo per finalità di *marketing* dei dati delle ricevitorie;
- 2 controlli nei confronti di compagnie di assicurazione, con riferimento all'utilizzo dei dati dei clienti per finalità di *marketing*;
- 2 controlli nei confronti di soggetti pubblici che utilizzano i sistemi informativi della fiscalità mediante "anagrafe tributaria", per verificare la liceità dei trattamenti e le misure di sicurezza adottate;
- 2 controlli nei confronti di enti previdenziali, volti a verificare la liceità dei trattamenti e le misure di sicurezza adottate;
- 2 controlli nei confronti di società che forniscono servizi informatici in modalità *cloud computing*, *hosting*, *housing* e *facility management*.

A questi si aggiungono 142 controlli effettuati nei confronti anche di altre categorie di soggetti, per esigenze istruttorie connesse a specifiche segnalazioni pervenute all'Autorità.

In relazione a quanto emerso dagli accertamenti, sono state effettuate numerose proposte di adozione di provvedimenti inibitori e/o prescrizioni per conformare il trattamento alla legge, a fronte delle quali l'Autorità ha adottato alcuni provvedimenti di particolare rilievo per le garanzie nei confronti dei cittadini.

Tra i più rilevanti, in ordine cronologico, si segnalano:

- il provvedimento con il quale il Garante ha vietato il trattamento di dati personali posto in essere da alcune società in relazione all'invio di fax promozionali, senza che fosse rilasciata l'informativa ai sensi dell'art. 13 del Codice e che risultasse la prova del consenso preventivo, specifico e informato degli interessati, ai sensi degli artt. 23 e 130 del Codice (provv. 2 marzo 2011 [doc. *web* n. 1802423]);

- il provvedimento con il quale il Garante ha disposto la cessazione dell'efficacia di un precedente divieto (adottato il 24 febbraio 2010) nei confronti di una società che opera nel settore manifatturiero, con riferimento ai trattamenti di dati dei dipendenti in occasione del loro allontanamento temporaneo dalla postazione di lavoro (provv. 31 marzo 2011 [doc. *web* n. 1807758]);
- il provvedimento con il quale il Garante ha vietato il trattamento dei dati di persone disabili utilizzati per l'invio di comunicazioni promozionali, in assenza del consenso specifico ed informato degli interessati, ai sensi degli artt. 13, 23 e 26 del Codice (provv. 31 marzo 2011 [doc. *web* n. 1810166]);
- il provvedimento con il quale il Garante ha vietato il trattamento dei dati posto in essere da una società tramite la costituzione e diffusione *online* di un elenco telefonico i cui dati non sono stati tratti dal *database* telefonico unico (DBU), utilizzato anche per la funzione di "ricerca inversa", in violazione del provvedimento 15 luglio 2004 (provv. 7 aprile 2011 [doc. *web* n. 1810351]);
- il provvedimento con il quale il Garante ha vietato il trattamento dei dati posto in essere da una società che, sebbene conservasse all'estero i dati personali e li gestisse in modalità remota, utilizzava in modo prevalente un apparato di rete (fax *gateway*) collocato sul territorio italiano per l'invio di comunicazioni promozionali senza il consenso degli interessati (provv. 7 aprile 2011 [doc. *web* n. 1810207]);
- i provvedimenti con i quali il Garante ha disposto il blocco dei trattamenti di dati posti in essere con sistemi di videosorveglianza, attraverso i quali era possibile effettuare un controllo a distanza dell'attività lavorativa dei dipendenti, senza l'accordo con le rappresentanze sindacali aziendali né in alternativa, la specifica autorizzazione da parte della direzione provinciale del lavoro (provv. 14 aprile 2011 [doc. *web* n. 1810223], provv. 10 novembre 2011 [doc. *web* n. 1859539], provv. 17 novembre 2011 [doc. *web* nn. 1859558 e 1859546].
- il provvedimento con il quale il Garante ha vietato il trattamento dei dati posto in essere da una società che inviava fax, e-mail ed sms con modalità automatizzate per conto di terzi rappresentati, nella maggior parte dei casi, *tour operator* che promuovevano "pacchetti vacanze" nei confronti di agenzie di viaggio (provv. 5 maggio 2011 [doc. *web* n. 1822815]);

- il provvedimento generale con il quale il Garante ha impartito al settore bancario prescrizioni in materia di circolazione delle informazioni e di tracciamento delle operazioni di accesso ai dati dei clienti (provv. 12 maggio 2011 [doc. *web* n. 1813953]);
- i provvedimenti con i quali il Garante ha vietato il trattamento dei dati posto in essere da società che comunicavano ad altri soggetti dati per l'invio di comunicazioni commerciali via sms, senza aver rilasciato agli interessati un'idonea informativa ai sensi dell'art. 13 del Codice e senza aver acquisito uno specifico consenso ai sensi dell'art. 23 del Codice stesso (provv. 10 giugno 2011 [doc. *web* n. 1836396]; provv. 26 ottobre 2011 [doc. *web* n. 1851750]);
- il provvedimento con il quale il Garante ha vietato il trattamento dei dati posto in essere da una società, senza aver fornito agli interessati un'idonea informativa ai sensi dell'art. 13 comma 4, del Codice e senza aver acquisito uno specifico consenso per l'invio, via sms, di comunicazioni promozionali automatizzate ai sensi dell'art. 130; i dati erano anche trasferiti all'estero in assenza di uno dei presupposti previsti dagli artt. 43 o 44 del Codice e, quindi, in violazione dell'art. 45 del Codice stesso (provv. 30 giugno 2011 [doc. *web* n. 1834208]);
- il provvedimento con il quale il Garante ha: dichiarato illeciti i trattamenti effettuati da una società in violazione degli artt. 113 e 114 del Codice nonché 4 e 8, l. n. 300/1970, con la conseguente inutilizzabilità dei dati trattati in violazione di legge, ai sensi dell'art. 11, comma 2, del Codice stesso; vietato la conservazione e la categorizzazione, su base individuale, dei dati personali riferiti alla navigazione internet dei dipendenti, nonché la conservazione dei dati relativi alle utenze telefoniche chiamate dai singoli dipendenti (provv. 21 luglio 2011 [doc. *web* n. 1829641]);
- il provvedimento con il quale il Garante ha vietato il trattamento posto in essere da un'università *online* dei dati (luogo e data di nascita, codice fiscale, cittadinanza) acquisiti mediante il form di registrazione al proprio sito, eccedenti rispetto alla dichiarata finalità del servizio di registrazione –di mantenimento dei contatti con gli utenti interessati al mondo dell'Ateneo e di informazione dei medesimi riguardo alle novità e agli appuntamenti dell'Ateneo stesso– in violazione dei princìpi di pertinenza e non eccedenza di cui all'art. 11 comma 1, lettera *d*) (provv. 7 settembre 2011 [doc. *web* n. 1844176] già cit. al par. 8.3.);

– il provvedimento con il quale il Garante ha accertato la effettiva titolarità del trattamento dei dati di una società fornitrice di servizi telefonici così detti "a valore aggiunto" (VAS), con riguardo alle operazioni di trattamento effettuate nei confronti di diversi operatori telefonici (provv. 15 settembre 2011 [doc. *web* n. 1849872]);

In molti dei provvedimenti sopra citati l'Autorità, accertata la violazione di norme del Codice per le quali la legge prevede una sanzione amministrativa, ha informato il destinatario dell'atto del successivo avvio del procedimento sanzionatorio.

In questi casi, quindi, successivamente alla notifica del provvedimento è stata formalizzata la contestazione delle violazioni nei confronti del soggetto individuato come responsabile.

## 17.4. L'ATTIVITÀ SANZIONATORIA DEL GARANTE

*17.4.1. Violazioni penali e procedimenti relativi alle misure minime di sicurezza*

A seguito delle ispezioni effettuate e, più in generale, dall'esame degli atti delle istruttorie svolte dall'Autorità, sono stati rilevati gli estremi per l'invio all'autorità giudiziaria di 37 informative (di cui 16 direttamente da parte dell'Autorità e 21 da parte della Guardia di finanza).

Le segnalazioni relative a presunte violazioni penali hanno riguardato:

– in 20 casi la mancata adozione delle misure minime di sicurezza;
– in 1 caso l'inosservanza di un provvedimento del Garante;
– in 2 casi la falsità nelle dichiarazioni e notificazioni al Garante;
– in 4 casi il trattamento illecito dei dati;
– in 10 casi violazioni della l. n. 300/1970 (Statuto dei lavoratori), punite come reato dall'art. 171 del Codice, o altre violazioni penali previste da disposizioni non contenute nel Codice in materia di protezione dei dati personali.

La violazione penale più segnalata riguarda, anche per l'anno 2011, il mancato rispetto delle disposizioni concernenti le misure minime di sicurezza che chi tratta dati personali (titolari, responsabili ed incaricati) deve adottare per assicurare il livello di sicurezza predefinito dalle norme. Tra queste può essere annoverata anche la designazione degli incaricati del trattamento, che non costituisce un mero adempimento formale, in quanto la

parte più significativa delle misure di sicurezza è strettamente correlata all'attività degli incaricati stessi (ovvero di coloro che ordinariamente operano sui dati personali, cfr. regole 1-10 (autenticazione informatica), 12-15 (adozione di un sistema di autorizzazione), 22 e 23 (dati sensibili contenuti in supporti rimovibili), 27 (dati comuni contenuti in supporti cartacei), 28 e 29 (dati sensibili contenuti in supporti cartacei) dell'Allegato B. al Codice) e mira a fornire loro istruzioni per il corretto trattamento dei dati, rendendoli al contempo consapevoli delle connesse responsabilità anche attraverso specifici processi formativi.

Tale adempimento assume peraltro maggiore significato alla luce dell'orientamento espresso della Corte di Cassazione Sezioni unite penali nella sentenza n. 4694/2012, con riferimento al reato di accesso abusivo a un sistema informatico o telematico, previsto dall'art. 615-*ter* del codice penale.

Secondo la Corte, infatti, *"integra la fattispecie criminosa di accesso abusivo ad un sistema informatico o telematico protetto, prevista dall'art. 615-ter c.p., la condotta di accesso o di mantenimento nel sistema posta in essere da soggetto che, pure essendo abilitato, violi le condizioni ed i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema per delimitarne oggettivamente l'accesso".*

Seguendo questo principio, si può ritenere che la delimitazione dell'ambito del trattamento consentito all'incaricato e la predisposizione di opportune prescrizioni (istruzioni all'incaricato nella terminologia corrente del Codice) possano costituire la linea di demarcazione rispetto a comportamenti che potrebbero quindi, in tale prospettiva, essere suscettibili di valutazione sotto il profilo penale.

Sotto il profilo procedurale, nel caso in cui venga rilevata l'omessa adozione di una o più misure minime di sicurezza (specificatamente previste dal Disciplinare tecnico sulle misure di sicurezza Allegato B. al Codice), in base al disposto dell'art. 169, comma 2, del Codice, il Garante impartisce una prescrizione alla persona individuata come responsabile della relativa violazione e, verificata la regolarizzazione, ammette il responsabile stesso al pagamento del quarto del massimo della sanzione prevista (pari a 30.000 euro). L'adempimento alla prescrizione ed il pagamento della somma, vengono comunicati all'autorità giudiziaria competente per le valutazione in ordine all'estinzione del reato.

Con riferimento a questa complessa procedura, i procedimenti definiti nell'anno 2011 connessi al cd. "ravvedimento operoso" in materia di misure minime di sicurezza, sono stati 12 e hanno determinato il pagamento all'Autorità di 432.500 euro da parte delle persone responsabili delle violazioni.

*17.4.2. Sanzioni amministrative*

A seguito delle ispezioni effettuate e delle istruttorie curate dall'Ufficio, sono stati avviati 358 procedimenti sanzionatori amministrativi.

Le sanzioni amministrative contestate hanno riguardato le seguenti violazioni:

- omessa o inidonea informativa (192);
- trattamento dei dati in violazione dell'art. 33 o delle disposizioni indicate nell'art. 167 (100);
- omessa informazione o esibizione al Garante (22);
- violazione del diritto di opposizione (21);
- omessa o incompleta notificazione (11);
- inosservanza di un provvedimento del Garante (11);
- più violazioni da parte di soggetti che gestiscono banche dati di particolare rilevanza e dimensioni (1).

I procedimenti sanzionatori definiti nell'anno sono stati 281 di cui 202 hanno comportato l'applicazione di una sanzione e 79 sono stati archiviati in quanto la parte ha potuto dimostrare di non aver commesso la violazione contestata o che la violazione non le era imputabile.

Come evidenziano i dati, il maggior numero di sanzioni irrogate ha riguardato la violazione dell'obbligo di fornire all'interessato tutte le informazioni riguardanti il trattamento dei dati, al fine di renderlo pienamente consapevole dell'effettivo utilizzo dei suoi dati personali, nonché la violazione dell'obbligo di acquisirne il consenso, spesso connessa a trattamenti illeciti per attività di *marketing*.

Per la prima volta sono state anche contestate le violazioni del diritto di opposizione all'utilizzo del proprio numero di telefono per finalità di *marketing*, manifestata attraverso l'iscrizione al Registro pubblico delle opposizioni (fattispecie introdotta all'art. 162, comma

2-*quater*, del Codice con il d.l. 25 settembre 2009, n. 135, convertito dalla l. 20 novembre 2009, n. 166). In tutti i casi nei quali, a seguito di segnalazioni degli interessati, è stato possibile accertare l'effettuazione di chiamate promozionali nei confronti di numerazioni iscritte al registro delle opposizioni, si è proceduto a contestare la violazione del predetto diritto, che prevede una pena pecuniaria da 10.000 a 120.000 euro.

Numerosissime sono le istruttorie già avviate in questo settore ed ancora in corso, sicché nell'anno 2012 il numero di sanzioni per violazione del diritto di opposizione appare destinato ad aumentare notevolmente.

Complessivamente, le entrate relative all'attività sanzionatoria per l'anno 2011 sono state pari a 3.073.430 euro, in relazione a:

- procedimenti sanzionatori spontaneamente definiti mediante pagamento da parte dei contravventori (per un importo di 1.810.400 euro);
- ordinanze-ingiunzione adottate dall'Autorità a seguito dell'esame delle memorie difensive e delle audizioni delle parti (per un importo di 830.530 euro);
- ammissioni al pagamento in relazione a procedimenti sulle misure minime di sicurezza (per un importo di 432.500 euro).

I proventi delle sanzioni applicate dal Garante sono devoluti allo Stato. Sulla base di quanto previsto dall'art. 166 del Codice, tali proventi, nella misura del 50% del totale annuo sono riassegnati al fondo stanziato per le spese di funzionamento dell'Autorità previsto dall'art. 156, comma 10, del Codice e sono utilizzati unicamente per l'esercizio della attività ispettiva e di divulgazione della disciplina della protezione dei dati personali.

*17.4.3. Alcuni princìpi rilevabili dalle ordinanze-ingiunzioni adottate dal Garante*

Dall'esame delle ordinanze-ingiunzioni adottate dal Garante e pubblicate sul sito è possibile desumere alcuni princìpi di carattere generale.

In un'ordinanza-ingiunzione emessa nei confronti di un'impresa che aveva effettuato un trattamento di dati biometrici per la rilevazione delle presenze dei propri dipendenti senza, tra l'altro, aver richiesto una verifica preliminare (art. 17 del Codice) e senza aver adottato le prescrizioni di cui al provvedimento del Garante "Linee-guida in materia di trattamento di

dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati" del 23 novembre 2006 [doc. *web* n. 1364099], si è posto il problema dell'eventuale congiunta applicabilità della sanzione prevista dall'art. 162, comma 2-*bis*, del Codice per inosservanza del citato art. 17 e di quella di cui all'art. 162, comma 2-*ter*, del Codice stesso per inosservanza di tale provvedimento.

Sulla base degli atti, l'Autorità ha rilevato l'insussistenza di "elementi per applicare la sanzione di cui all'art. 162, comma 2-*ter*", del Codice; in quanto l'utilizzo di un sistema di rilevazione delle presenze basato sul trattamento di dati biometrici dei dipendenti, in un'ipotesi non contemplata dal suddetto provvedimento del 2006, comportava la necessità di richiedere una verifica preliminare ai sensi del citato art. 17, per la cui omissione veniva applicata la sanzione prevista dall'art. 162, comma 2-*bis*, del Codice stesso.

Rilevante anche il principio affermato nella stessa ordinanza-ingiunzione, relativamente all'obbligo di notificazione al Garante di cui all'art. 37, comma 1, del Codice. L'Autorità ha evidenziato che l'omessa notificazione "sostanzia un illecito omissivo di natura permanente, per il quale il momento della consumazione coincide con la cessazione della condotta (effettuazione della notificazione) ovvero con il momento in cui la violazione viene accertata". Ne consegue che il momento in cui la condotta eventualmente cessa, in quanto il soggetto tenuto alla notificazione ancorché in ritardo vi ha provveduto, coincide con il momento della consumazione dell'illecito cui fare riferimento per individuare la norma sanzionatoria applicabile e il termine di decorrenza della prescrizione (ordinanza-ingiunzione 10 giugno 2011 [doc. *web* n. 1859107]).

In un altro caso è stato affrontato un aspetto procedurale circa il rispetto dei termini dell'istruttoria. Al riguardo occorre evidenziare come le norme che regolano i termini dell'istruttoria preliminare dei procedimenti amministrativi del "reclamo" e della "segnalazione" sono contenute negli artt. 11, comma 1 e 14, comma 2, del regolamento del Garante n. 1/2007. I termini relativi al distinto e autonomo procedimento sanzionatorio amministrativo sono, invece, disciplinati dalla l. n. 689/1981, come peraltro indicato nella Tabella A, del regolamento del Garante n. 2/2007. Nel provvedimento l'Autorità afferma che: "l'istruttoria preliminare del procedimento sanzionatorio è volta all'accertamento della violazione

amministrativa ovvero alla valutazione dei dati acquisiti ed afferenti agli elementi costitutivi, sia soggettivi che oggettivi, dell'infrazione. Sul punto, il costante orientamento della giurisprudenza ha ormai reso pacifico il fatto che l'attività di accertamento dell'illecito amministrativo deve essere intesa come comprensiva del tempo necessario alle valutazioni anzidette (*ex multis*, Cass. civ. Sez. II, 30 maggio 2006, n. 12830), senza, quindi, prevedere alcun termine perentorio" (ordinanza-ingiunzione 16 febbraio 2011, [doc. *web* n. 1855692]).

# 18. LE RELAZIONI INTERNAZIONALI

## 18.1. LE CONFERENZE DELLE AUTORITÀ SU SCALA INTERNAZIONALE

Conferenza internazionale delle autorità di protezione dati Città del Messico 2011

La 33ª Conferenza internazionale delle autorità di protezione dei dati si è svolta a Città del Messico il 2 e il 3 novembre 2011 con il titolo *"Privacy: The Global Age"*. Nella sessione dedicata esclusivamente alle autorità di protezione dati sono state approvate tre risoluzioni, riguardanti:

- la protezione dei dati personali nel contesto di eventi naturali di particolare gravità; risoluzione proposta dall'autorità della Nuova Zelanda, che incoraggia una riflessione sulla flessibilità della protezione dei dati in funzione della salvaguardia degli interessi vitali delle persone in caso di disastro naturale;
- il rafforzamento dei meccanismi di cooperazione delle autorità in ambito internazionale a fini di *"enforcement"*; risoluzione proposta dai *Commissioners* di Regno Unito e Canada, che istituisce un gruppo di lavoro all'interno della Conferenza per definire un quadro legale ed i possibili meccanismi di coordinamento tra le autorità anche allo scopo di scambiare le informazioni relative a casi di indagini in corso o potenziali;
- l'uso di un identificatore unico nell'impiego del Protocollo internet versione 6 (IPv6); risoluzione proposta dall'autorità tedesca, che raccomanda di mantenerne l'uso anche con l'introduzione del nuovo protocollo di indirizzi temporanei (*dynamic addresses*), *'by default'*.

La Conferenza è stata principalmente dedicata all'esame delle modalità di tutela effettiva e non burocratica della protezione dei dati personali in un contesto in cui lo sviluppo delle tecnologie, le nuove forme di comunicazione in rete, la proliferazione dei dati, l'uso innovativo delle informazioni, hanno aperto orizzonti finora impensabili e al tempo stesso comportato grandi sfide e rischi per i diritti delle persone. Nella consapevolezza della necessità di un approccio globale ai menzionati problemi, si è discusso, in particolare, della sicurezza delle informazioni e della notifica dei cd. *data breaches*, del *cloud computing*, del diritto all'oblio nel mondo digitale, della ridefinizione del concetto di dato personale in relazione agli scenari aperti dalla rete, della necessità di regole riconosciute a livello internazionale.

Nella *"Closed Session"* le autorità hanno inoltre discusso i rapporti del comitato esecutivo sulle modalità di organizzazione delle conferenze internazionali ed il rapporto del comitato per l'accreditamento, accettando le richieste di partecipazione –in qualità di membri– delle autorità della Bosnia Erzegovina e del Marocco –e quali osservatori– di Giappone, Macao, Perù (quest'ultimo a partire dal prossimo anno) e Corea del Sud (per la quale non è ancora stata provata la sussistenza del requisito di indipendenza dell'autorità).

È stato anche dato il benvenuto all'Uruguay, che si è offerto di organizzare la Conferenza internazionale del 2012.

*Spring Conference* 2011

La *Spring Conference* del 2011, tenutasi a Bruxelles il 5 aprile, ha adottato una risoluzione che ha evidenziato l'esigenza di un approccio globale alla protezione dei dati personali, più idoneo a configurarla quale diritto fondamentale della persona. La Conferenza si è anche occupata della definizione di una politica europea comune in materia di supervisione nel settore della cooperazione giudiziaria e di polizia, sulla base di un documento predisposto dal Garante europeo per la protezione dei dati, oggetto di ampia discussione e che ha condotto nei mesi successivi alla redazione di un ulteriore e più articolato documento da sottoporre alla *Spring Conference* del 2012 per l'approvazione.

Una specifica sessione è stata dedicata al futuro del *Working Party on Police and Justice* (*Wppj*) alla luce del Trattato di Lisbona e dell'opportunità di garantire un'efficace ripartizione delle competenze fra i soggetti incaricati della supervisione (visto che il Gruppo Art. 29 dell'Ue sarà chiamato necessariamente ad occuparsi delle questioni *ex*-III pilastro). È emersa una netta preferenza per la graduale integrazione nelle attività svolte dal *Wppj* delle materie dell'*ex*-III pilastro, con il sostegno degli attuali presidente e vice-presidente del Gruppo stesso.

La Conferenza ha inoltre accettato le richieste di partecipazione dell'Autorità della Repubblica Moldava e dell'Autorità comune di controllo (ACC) di EUROJUST (senza diritto di voto).

### 18.2. LA COOPERAZIONE TRA AUTORITÀ GARANTI NELL'UE: IL GRUPPO ART. 29

Il Gruppo Art. 29, mantenendo il suo ruolo di attivo interlocutore delle istituzioni comunitarie, *in primis* della Commissione europea, ha contribuito al dibattito sull'attualità della

Direttiva n. 95/46/CE e della Decisione quadro 2008/977/GAI del Consiglio dell'Ue, nonché ai lavori preparatori della revisione di tale normativa, che si sono conclusi con la presentazione, il 25 gennaio 2012, del nuovo "pacchetto di riforma" sul trattamento dei dati personali.

Parere 12/2011 sul concetto di consenso

Tale impegno risulta dal programma di lavoro 2010-2011 (WP 170), del quale si è riferito nella Relazione 2010 (v. p. 211) e sulla cui base sono stati adottati diversi pareri e documenti.

Il parere approvato il 13 luglio 2011 (WP 187), sul tema del consenso dell'interessato, relativo anche all'applicazione degli artt. 7, 8 e 26 della Direttiva n. 95/46/CE, fornisce alla Commissione alcune proposte in vista della revisione della direttiva stessa.

In particolare, è stato suggerito di: chiarire il concetto di "inequivocabilità" del consenso, onde evitare che il "silenzio" possa essere considerato un consenso valido; introdurre espressamente il diritto di "revoca" del consenso; enfatizzare i requisiti del consenso "informato" e "preventivo"; con riferimento ai soggetti incapaci, individuare chiaramente in quali circostanze il consenso possa essere manifestato dai genitori o dal rappresentante legale del soggetto incapace e, nel caso di minori, rendere obbligatorio l'uso di meccanismi di verifica dell'età del soggetto.

Lettera del Gruppo alla Commissione europea del 20 aprile 2011

Il Gruppo ha inoltre adottato alcuni documenti quali *"advice paper"*, per sottoporre alla Commissione europea, senza pretese di esaustività, alcune proposte di modifica della normativa, su tre questioni di particolare interesse: i dati sensibili, la semplificazione degli obblighi di notificazione, la cooperazione tra le autorità di protezione dei dati personali.

I documenti sono accompagnati da una lettera alla Commissione (20 aprile 2011), che indica le soluzioni che hanno ottenuto la maggioranza dei consensi. In particolare, per i dati sensibili, il divieto di trattamento con lista "chiusa", salvo eccezioni. In materia di notificazione, un sistema basato su una "lista positiva" di trattamenti per i quali è necessaria la notificazione, analogamente al modello italiano. In materia di cooperazione, è stato posto l'accento sull'esigenza di maggiore armonizzazione relativamente ai poteri, alle competenze e all'indipendenza delle autorità di protezione dei dati personali.

Nella lettera viene, infine, rappresentata l'opportunità che i *paper* in questione siano letti insieme al parere del Gruppo in materia di revisione della direttiva (WP 168 del 1° dicembre 2009), alla lettera trasmessa dal Gruppo alla Commissaria Reding il 14 gennaio 2011 (*Letter*

*from the Article 29 Working Party addressed to Vice-President Reding regarding the Article 29 WP's reaction to the Commission Communication 'A comprehensive approach to personal data protection in the EU'*) e al parere sulla legge applicabile (WP 179 del 16 dicembre 2010), esortando la Commissione a riflettere sulla scelta di soluzioni che evitino il ricorso al *"forum shopping"* in materia di protezione dei dati personali.

Sempre in linea con il programma di lavoro 2010-2011, il Gruppo ha dedicato particolare attenzione alle cd. "sfide tecnologiche" per la protezione dei dati, sia in relazione alla revisione della Direttiva n. 2002/58/CE, operata attraverso le Direttive nn. 2009/136/CE e 2009/140/CE, fornendo chiarimenti interpretativi ed operativi sull'applicazione della norma di nuova introduzione relativa alla "notifica delle violazioni di dati" (art. 4, par. 3 della Direttiva n. 2002/58/CE aggiunto dalla Direttiva n. 2009/136/CE) (WP 184 del 5 aprile 2011) sia commentando il codice di autodisciplina proposto dall'*International Advertising Bureau* (*IAB*), al fine di regolamentare l'utilizzo di *cookies* per tracciare la navigazione degli utenti di internet allo scopo di proporre pubblicità mirata (*targeted advertising*) (WP 188 dell'8 dicembre 2011).

Parere 1/2011 sul quadro regolamentare applicabile ai *data breach*

Nel parere relativo all'obbligo di notifica delle violazioni dei dati (*data breach notification*), il Gruppo ha sottolineato la necessità di armonizzare gli atti nazionali di recepimento (previsti dalla Direttiva entro il 25 maggio 2011), stabilire criteri di notifica dei *data breach*, con particolare riferimento agli aspetti tecnico-operativi (tempi di notifica, soglie di gravità, canali di comunicazione) ed assicurare la coerenza, anche terminologica, tra i provvedimenti normativi previsti per il recepimento delle modifiche della direttiva *e-privacy* e gli atti di trasposizione della Direttiva n. 95/46/CE. Si tratterrà di raccogliere le informazioni ed esperienze nazionali in vista della creazione della "Piattaforma" di lavoro comune menzionata nel documento, anche ai fini della cooperazione con gli altri soggetti competenti per la definizione degli specifici meccanismi attuativi (Agenzia europea per la sicurezza delle reti e dell'informazione-ENISA, Garante europeo della protezione dei dati, Commissione europea).

Parere 16/2011 sulle raccomandazioni EASA/IAB sulla pubblicità comportamentale *online*

Nel parere sulla pubblicità comportamentale e protezione dei dati personali *online* (WP 188 dell'8 dicembre 2011), il Gruppo, concentrandosi sui princìpi del consenso e dell'informativa, precondizioni essenziali alla valutazione della legittimità del trattamento, è giunto