dell'attività del personale incaricato di accedere ai dati; la conservazione separata dei dati e la loro cancellazione una volta decorso il termine di conservazione stabilito dalla legge; l'effettuazione di controlli interni sulla legittimità degli accessi ai dati da parte degli incaricati e l'adozione di sistemi di cifratura;

- operano nel settore del credito, per verificare il trattamento di dati personali relativi all'utilizzo di impianti di videosorveglianza, sia di tipo tradizionale che di tipo integrato con la rilevazione di dati biometrici della clientela (tratti dall'analisi delle impronte digitali). In tali casi le verifiche si sono incentrate sull'utilizzo di sistemi di videosorveglianza, per accertare il rispetto di quanto prescritto dal Garante nell'ambito del provvedimento generale in materia di videosorveglianza dell'8 aprile 2010 (doc. web n. 1712680); sull'utilizzo di sistemi di videosorveglianza integrati con la raccolta delle impronte digitali della clientela, al fine di verificare, in particolare, la sussistenza dei presupposti di liceità del trattamento e l'adozione delle misure di tutela previste dal provvedimento generale 27 ottobre 2005 (doc. web n. 1246675), tra cui: nomina del "vigilatore" dei dati, ottenimento dell'attestato di conformità di cui alla regola n. 25 dell'All. B al Codice, rispetto dei tempi massimi di conservazione e delle procedure di cancellazione automatica dei dati, adozione di sistemi di cifratura "robusti", affissione di una informativa "minima" all'esterno dell'agenzia, effettiva predisposizione di modalità alternative di accesso per la clientela;
- sviluppano o distribuiscono applicazioni per dispositivi mobili di comunicazione (cd. *app*) per rilevare: i trattamenti di dati personali effettuati e le modalità attraverso le quali viene resa l'informativa agli interessati; la tipologia di dati raccolti al momento della registrazione dell'interessato al servizio e, successivamente, al momento dell'istallazione dell'*app* sul dispositivo e durante il suo effettivo utilizzo;
- operano nel settore del *marketing*, con particolare riferimento ai trattamenti relativi alla profilazione degli interessati (cd. *market profiling*). In questo caso le verifiche hanno riguardato la tipologia dei dati raccolti, la completezza delle informative fornite agli interessati, la correttezza delle modalità utilizzate per raccogliere il consenso nonché l'effettuazione della notificazione del trattamento;
- operano avvalendosi dell'attività degli informatori scientifici del farmaco, per verificare, in particolare: l'origine dei dati personali relativi agli operatori sanitari contattati dalle cause farmaceutiche attraverso gli informatori scientifici, le modalità di raccolta degli stessi, l'eventuale profilazione, le modalità di rilascio dell'informativa e di acquisizione del consenso, nonché la titolarità delle banche dati costituite attraverso l'espletamento della suddetta attività. Tali verifiche, tuttora in corso, coinvolgono anche gli stessi informatori scientifici, sia nel caso in cui questi collaborino con la società farmaceutica in virtù di uno specifico mandato di agenzia, che nel caso in cui siano dipendenti della società stessa;
- gestiscono concessionarie "plurimarca" per la vendita di motoveicoli od operano nel settore del commercio elettronico (*e-commerce*), al fine di appurare il rispetto della disciplina con particolare riferimento ai profili dell'informativa resa agli interessati nonché del consenso dagli stessi manifestato, ove necessario;
- operano nel settore della compravendita di metalli preziosi o gioielli (cd. compro oro), al fine di appurare il rispetto della disciplina con particolare

riferimento ai profili dell'informativa resa agli interessati nonché al consenso degli stessi, ove necessario;
- operano nel settore alberghiero con strutture di categoria elevata o di lusso, al fine di verificare la liceità del trattamento dei dati della clientela, anche con riferimento ai dati raccolti attraverso siti web o attraverso l'utilizzo di sistemi di videosorveglianza, con particolare evidenza per le modalità di rilascio dell'informativa e di raccolta del consenso degli interessati, ove necessario;
- operano nel settore dei laboratori di analisi cliniche. In tal caso le verifiche hanno riguardato, oltre al rispetto delle disposizioni del Codice concernenti il rilascio dell'informativa, la raccolta del consenso e la notificazione del trattamento, anche l'analisi delle misure di sicurezza adottate per la protezione dei dati sensibili presenti presso i laboratori e di quelle predisposte per consentire agli interessati l'accesso ai propri dati personali via internet o per le comunicazioni attraverso l'uso della posta elettronica.

Particolarmente rilevante, per complessità e significatività di risultato, è stata l'attività condotta nei confronti dei principali nodi d'interscambio internet (*Internet eXchange Point*-IXP). I nodi di interscambio (d'ora in poi IXPs) sono infrastrutture fisiche che permettono a diversi internet *Service Providers* (ISPs) di scambiare traffico internet fra loro, interconnettendo le proprie reti IP (*Internet Protocol*) attraverso cd. accordi di *peering* (nelle reti informatiche, *peering* è l'interconnessione volontaria tra reti internet che siano distinte amministrativamente allo scopo di scambiare traffico fra gli utenti di entrambe). Questo consente agli ISPs risparmi sugli acquisti di banda trasmissiva fornita dagli *upstream provider* e maggiore efficienza e affidabilità.

In estrema sintesi, lo scopo principale di un IXP è di permettere alle reti degli ISPs, attraverso il punto di interscambio neutrale, di interconnettersi fra di loro direttamente, senza passaggi intermedi, piuttosto che far transitare il traffico attraverso uno o più *provider* esterni. Oltre agli evidenti benefici economici e gestionali, la connessione diretta tra gli operatori tramite un IXP diminuisce la "distanza" tra le reti degli ISPs nazionali (intesa quale numero di passaggi per connettere un ISP ad un altro), evitando che l'interconnessione avvenga, come spesso accade, al di fuori del territorio nazionale, con l'effetto di migliorare il servizio reso all'utenza internet poiché i tempi di latenza nelle comunicazioni basate su protocollo Ip tra utenti (aziende, individui) basati sul territorio nazionale saranno in genere inferiori, rendendo la fruizione dei servizi di rete più efficiente e rapida. Gli accordi di *peering* tra i partecipanti ad un nodo di interscambio sono per lo più effettuati a titolo gratuito e regolati in modo da garantire il rispetto del principio di neutralità dell'attività dell'IXP nei confronti degli afferenti.

L'attività di controllo nei confronti degli IXPs si inquadra nelle attività di controllo che l'Autorità effettua per verificare il rispetto delle disposizioni del Codice che disciplinano le comunicazioni elettroniche. Le ispezioni hanno messo in luce rilevanti criticità con riferimento a diversi profili attinenti la sicurezza.

Come richiesto dall'Autorità a seguito delle ispezioni, gli IXPs hanno introdotto adeguati sistemi di tracciamento delle attività svolte dai tecnici sugli apparati, in modo da rilevare eventuali anomalie, come la possibile deviazione o duplicazione del traffico internet, oppure il collegamento di altri apparati elettronici alla rete interna; hanno eliminato le credenziali tecniche "condivise", così da poter identificare con certezza le attività svolte dal singolo operatore o amministratore di sistema e adottato meccanismi di *audit* e *alert* per prevenire o scoprire eventuali attività "ostili"; hanno migliorato, inoltre, la sicurezza fisica dei locali, essendo stato rafforzato il controllo degli accessi e la sorveglianza dei locali tecnici, con particolare

attenzione anche alle infrastrutture e ai *data center*. Per quanto riguarda questo ultimo aspetto, l'Autorità ha raccomandato, agli IXPs che hanno parte dei loro apparati dislocati in *data center* esterni, di operare controlli attivi e regolari sulle strutture che li ospitano.

Il Garante, consapevole del fatto che la sicurezza delle comunicazioni elettroniche coinvolge le competenze anche di altri soggetti istituzionali, ha dato notizia delle attività svolte al Presidente del Consiglio, trasmettendo altresì il rapporto ispettivo, affinché fosse valutato dagli organismi preposti alla sicurezza cibernetica del Paese (nota 26 maggio 2014). Alla segnalazione del Garante ha fatto seguito un'attività del Nucleo per la sicurezza cibernetica della Presidenza del Consiglio dei ministri, nell'ambito della quale sono state individuate plurime linee di azione per aumentare la sicurezza delle reti.

Sono stati effettuati altresì controlli nei confronti di singoli titolari del trattamento per esigenze istruttorie connesse alle segnalazioni, ai reclami e ai ricorsi pervenuti 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, come riportato nel prossimo paragrafo, ha adottato alcuni provvedimenti particolarmente significativi per i cittadini.

22.4. *I provvedimenti adottati dall'Autorità a seguito dell'attività ispettiva*

Attraverso le ispezioni l'Autorità svolge una penetrante attività istruttoria che può essere finalizzata, a seconda del caso, a uno o più dei seguenti obiettivi:

- intervenire sui trattamenti illeciti da chiunque effettuati adottando i provvedimenti cautelari previsti dalla legge (blocco e divieto) e/o definendo le misure necessarie da prescrivere per rendere il trattamento conforme alla legge (contrasto dell'illecito);
- verificare lo stato di attuazione delle prescrizioni adottate dal Garante nei diversi contesti e sanzionare gli eventuali inadempimenti al fine di prevenire futuri illeciti (attività preventiva);
- acquisire tutti gli elementi utili a comprendere nuovi fenomeni emergenti suscettibili di incidere significativamente sul diritto alla protezione dei dati personali (ad es., il tema del *mobile remote payment*) in modo da definire tempestivamente misure e accorgimenti da adottare (attività conoscitiva).

Occorre tenere presente che, al di là della/e finalità che la sottendono, l'ispezione è comunque pur sempre un procedimento amministrativo di controllo all'esito del quale, ove vengano accertate illiceità, l'Autorità è tenuta ad adottare i necessari provvedimenti per rendere il trattamento conforme alla legge e a contestare le sanzioni eventualmente rilevate.

Con riferimento al 2014, tra i provvedimenti più rilevanti adottati sulla base degli elementi istruttori acquisiti in sede ispettiva si segnalano, in ordine cronologico, i provvedimenti con i quali il Garante ha:

- dichiarato illecito il trattamento dei dati personali effettuato mediante un sistema di videosorveglianza da titolari del trattamento, pubblici e privati, in assenza dell'accordo con le rappresentanze sindacali e dell'autorizzazione del competente ufficio periferico del Ministero del lavoro, in violazione quindi degli artt. 114 del Codice e 4, l. n. 300/1970 (provv.ti 9 gennaio 2014, n. 13, doc. web n. 2927804 e 4 dicembre 2014, n. 559, doc. web n. 3671057);
- rilevato l'illiceità del trattamento effettuato dalla Società italiana di nefrologia per l'alimentazione del Registro italiano di dialisi e trapianto in man-

canza dell'informativa e del consenso dei pazienti interessati (artt. 13, 23, 106, 107 e 110 del Codice) e vietato all'associazione medesima di effettuare per il futuro ulteriori trattamenti di dati personali anche attinenti alla salute, salva l'adozione delle misure necessarie indicate dal Garante (provv. 16 gennaio 2014, n. 16, doc. web n. 2937031);

- dichiarato illecito il trattamento dei dati personali di imprese e professionisti effettuato da una società che inviava fax promozionali, senza la preventiva acquisizione del necessario consenso libero, informato, specifico e documentato per iscritto *ex* artt. 23, comma 3 e 130, commi 1 e 2, del Codice (provv. 23 gennaio 2014, n. 30, doc. web n. 2927848);
- disciplinato il fenomeno delle cd. chiamate mute, nelle quali cioè la persona contattata, dopo aver attivato il ricevitore, non viene messa in comunicazione con alcun interlocutore, e la cui ricezione reiterata e continua, a volte anche per dieci - quindici volte di seguito e spesso protratta nel tempo, determina un particolare disturbo ai destinatari ai quali, in difetto appunto di interlocutore, sono preclusi tutele e rimedi. Il provvedimento, avente carattere generale, prescrive ai titolari del trattamento che utilizzano i *call center* misure atte a minimizzare questo fenomeno (provv. 20 febbraio 2014, n. 83, doc. web n. 3017499);
- impartito specifiche prescrizioni a società esercenti l'attività di fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazione, in relazione alla verifica del mancato rispetto delle misure e degli accorgimenti da adottare a garanzia degli interessati, con riferimento ai dati di traffico telefonico e telematico conservati per finalità di accertamento e repressione dei reati (cd. *data retention*), già prescritti dall'Autorità con il provv. generale 17 gennaio 2008 (doc. web n. 1482111), successivamente integrato con il provv. generale 24 luglio 2008 (doc. web n. 1538237) (provv.ti 20 febbraio 2014, n. 84, doc. web n. 3031194 e 20 marzo 2014, n. 137, doc. web n. 3136961);
- prescritto a un'azienda sanitaria le misure per rendere conformi al Codice i trattamenti effettuati dagli interessati in relazione alle operazioni di pagamento dei corrispettivi per le prestazioni sanitarie dalla stessa erogate attraverso la rete Sportello amico di Poste Italiane s.p.a. e tramite il proprio sito internet (provv. 13 marzo 2014, n. 120, doc. web n. 3041470);
- prescritto ai titolari che effettuano trattamenti di dati personali nell'ambito delle operazioni di *mobile remote payment*, le misure per effettuare tali trattamenti nel rispetto dei principi generali di liceità, pertinenza, non eccedenza, correttezza e buona fede di cui all'art. 11 del Codice (provv. 22 maggio 2014, n. 258, doc. web n. 3161560);
- ritenuto illecito il trattamento effettuato da una società a mezzo del sistema di localizzazione dei veicoli aziendali volto a migliorare la qualità del servizio, a gestire i reclami degli utenti nonché a ottemperare a quanto richiesto da una regione in sede di affidamento del servizio, che consentiva altresì di effettuare il controllo a distanza dell'attività dei dipendenti che prestano servizio a bordo dei veicoli aziendali, senza che fossero attivate le procedure previste dall'art. 4, comma 2, l. 20 maggio 1970, n. 300; sono state inoltre prescritte le misure per rendere il trattamento conforme al Codice (provv. 2 ottobre 2014, n. 434, doc. web n. 3534543);
- rilevato l'illiceità del trattamento effettuato da due aziende sanitarie con riferimento all'omessa informativa e alla mancata acquisizione del consenso dell'interessato in relazione al trattamento dei dati dei pazienti effettuato

tramite il *dossier* sanitario aziendale (artt. 13, 23 e 76 e ss. del Codice), vietato ulteriori trattamenti di dati personali mediante lo strumento del *dossier* sanitario aziendale e prescritto le misure necessarie per rendere il trattamento dei dati conforme al Codice (provv.ti 23 ottobre 2014, n. 468, doc. web n. 3570631; 18 dicembre 2014, n. 610, doc. web n. 3725976);

- dichiarato illecita la raccolta dei dati personali degli utenti effettuata da una società sul proprio sito web e mediante moduli cartacei per le attività di invio di comunicazioni promozionali per conto proprio e/o per conto terzi nonché di comunicazione dei dati raccolti a soggetti terzi per le loro finalità promozionali (o comunque per finalità diverse da quelle strumentali ovvero collegate all'erogazione del servizio o dell'esecuzione del contratto), senza aver provveduto alla previa acquisizione del necessario consenso, *ex* art. 23, comma 3, del Codice; vietato il trattamento dei dati raccolti in violazione del Codice e prescritto alla medesima società le misure necessarie e opportune al fine di rendere il trattamento dei dati personali conforme alle disposizioni del Codice (provv. 20 novembre 2014, n. 532, doc. web n. 3657934).

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 avviato anche un procedimento sanzionatorio. In diversi casi inoltre l'Autorità, rilevando condotte punite come reato, ha disposto anche la trasmissione degli atti alla competente Procura della Repubblica.

22.5. *L'attività sanzionatoria del Garante*

22.5.1. Le violazioni penali e i procedimenti relativi alle misure minime di sicurezza

Nel 2014, in relazione alle istruttorie effettuate, sono state inviate 39 segnalazioni di violazioni penali all'autorità giudiziaria (cfr. sez. IV, tab. 7) di cui:

- venti per la mancata adozione delle misure minime di sicurezza;
- sette per violazioni della l. n. 300/1970 (Statuto dei lavoratori), ora punite come reato dall'art. 171 del Codice;
- due per falsità nelle dichiarazioni e notificazioni al Garante;
- una per trattamento illecito dei dati;
- una per inosservanza di un provvedimento del Garante;
- otto in relazione ad altre violazioni penali.

Come dimostrano i dati sopra riportati, permangono numerose le violazioni delle misure minime di sicurezza; ciò nonostante si tratti di adempimenti di non particolare complessità, in vigore da più di dieci anni, che dovrebbero essere stati oramai "metabolizzati" sia dalle imprese che dagli enti pubblici. Anche alla luce dell'esperienza maturata dall'Autorità in sede di controllo deve essere nuovamente segnalata la ormai indifferibile esigenza di aggiornare il "Disciplinare tecnico in materia di misure minime di sicurezza", All. B al Codice in vigore dal 2003, le cui prescrizioni appaiono in buona parte non più adeguate allo stato dell'evoluzione tecnica. Tale revisione dovrebbe essere ispirata a criteri di semplificazione, rispetto ad adempimenti di natura prettamente burocratica oggi previsti dalle disposizioni, e di maggiore effettività delle misure, prevedendo adeguati accorgimenti tecnici che intervengano in modo progressivo in funzione della quantità e della qualità dei dati, nonché della complessità della struttura tecnologica utilizzata e del numero di incaricati che vi hanno accesso. In questo senso, in data 22 settembre 2014 (doc. web n. 3531329), l'Autorità ha fatto una segnalazione al Presidente del Consiglio dei

ministri nell'ambito di una articolata proposta di semplificazione del quadro sanzionatorio e delle misure minime di sicurezza previste dal Codice (cfr. par. 22.7).

Al di là dei risvolti sanzionatori, occorre sottolineare che la mancata osservanza delle disposizioni relative alle misure minime di sicurezza è particolarmente grave perché espone i dati personali degli interessati al pericolo di accesso da parte di persone non autorizzate e a trattamenti non consentiti.

Sotto il profilo procedurale, nel caso in cui venga rilevata una violazione di una o più misure minime di sicurezza (specificatamente previste dal Disciplinare tecnico sulle misure di sicurezza All. 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 predetta violazione e, successivamente, verificato il ripristino delle misure violate, ammette il destinatario della prescrizione 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 valutazioni in ordine all'estinzione del reato.

In questo ambito merita segnalare la recente sentenza della Corte di Cassazione (Sez. pen., III, 16 gennaio 2015, n. 1986) che ha affrontato, respingendola, la questione di legittimità costituzionale dell'art. 169 del Codice, in riferimento agli artt. 2, 3, 21, 24, 25 della Costituzione. Nella motivazione si legge che "non sussiste, infatti, alcun contrasto di tale disposizione con gli artt. 3 e 24 Cost., perché rientra in generale nella piena discrezionalità del legislatore la fissazione dell'ammontare dell'oblazione ai fini dell'estinzione del reato, come avvenuto, attraverso il richiamo all'art. 162, comma 2-*bis*, in ragione di euro 30.000".

Nella stessa sentenza la Suprema Corte afferma, con riferimento alla responsabilità penale, che la stessa "è stata, del resto, positivamente accertata dalla Guardia di finanza nel corso delle indagini preliminari, attraverso l'accertamento diretto della mancata designazione dell'incaricato del trattamento in relazione ad un sito internet nel quale era possibile la raccolta di dati personali sensibili relativi a una serie indeterminata di persone", confermando la linea costantemente seguita negli anni dall'Autorità circa le conseguenze penali derivanti dall'omessa designazione degli incaricati del trattamento dei dati.

Anche nel 2014 si è avuta una rilevante incidenza dell'accertamento di violazioni penali relative allo Statuto dei lavoratori connesse, nella maggior parte dei casi, all'installazione di sistemi di videosorveglianza in assenza delle garanzie previste dall'art. 4, comma 2, l. n. 300/1970. Occorre tenere presente che la disciplina prevista dallo Statuto e relativa all'utilizzo di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori (art. 4) e al divieto di indagini sulle opinioni ai fini dell'assunzione (art. 8), costituisce parte integrante delle disposizioni del Codice (artt. 113 e 114) ed è sanzionata dall'art. 171.

22.5.2. Le sanzioni amministrative

Sono stati avviati n. 577 nuovi procedimenti sanzionatori amministrativi (cfr. sez. IV, tab. 6). All'accertamento delle violazioni amministrative previste dal Codice può procedere:

- il personale dell'Ufficio addetto all'attività ispettiva a cui, sulla base di quanto previsto dall'art. 156, comma 9, del Codice, nei limiti del servizio cui è destinato e secondo le rispettive attribuzioni, è attribuita la qualifica di ufficiale o agente di polizia giudiziaria;
- chiunque rivesta, nell'esercizio delle proprie funzioni, la qualifica di ufficiale o agente di polizia giudiziaria, in base a quanto previsto dall'art. 13, l. 24 novembre 1981, n. 689.

L'art. 13, l. n. 689/1981 prevede: "Gli organi addetti al controllo sull'osservanza delle disposizioni per la cui violazione è prevista la sanzione amministrativa del pagamento di una somma di denaro possono, per l'accertamento delle violazioni di rispettiva competenza, assumere informazioni e procedere a ispezioni di cose e di luoghi diversi dalla privata dimora, a rilievi segnaletici, descrittivi e fotografici e ad ogni altra operazione tecnica [...]. All'accertamento delle violazioni punite con la sanzione amministrativa del pagamento di una somma di denaro possono procedere anche gli ufficiali e gli agenti di polizia giudiziaria".

I procedimenti sanzionatori iniziano, pertanto, con la contestazione in relazione ad istruttorie effettuate direttamente dall'Autorità ma anche sulla base di accertamenti effettuati autonomamente da corpi dello Stato quali la Guardia di finanza, i Carabinieri, la Polizia di Stato ecc. che possono accertare le violazioni amministrative in materia di protezione dei dati personali in occasione di attività svolte sulla base dei propri poteri, anche di polizia giudiziaria. Questo "doppio binario" risulta complessivamente efficace, considerata l'amplissima platea di soggetti tenuti all'osservanza delle regole previste dal Codice, che renderebbe velleitario un sistema di accertamento delle violazioni accentrato solo nell'Autorità.

L'assicurazione di una uniformità di giudizio e di interpretazione è peraltro assicurata, in quanto la legge affida al solo Garante il compito dell'applicazione delle sanzioni in tutti i casi nei quali, a seguito dell'accertamento, il contravventore, non avvalendosi della possibilità di definire il procedimento con il pagamento entro sessanta giorni dalla notifica del doppio del minimo della sanzione, decida di proseguire il procedimento medesimo inviando scritti difensivi o chiedendo l'audizione. In tutti questi casi è infatti l'Autorità a prendere la decisione circa l'applicazione della sanzione adottando l'atto finale dell'ordinanza ingiunzione, quantificandone l'importo, o l'archiviazione.

Le violazioni in relazione alle quali sono stati avviati procedimenti sanzionatori nel 2014 hanno riguardato:

- l'omessa o inidonea informativa – art. 161 (n. 228);
- il trattamento illecito amministrativo – art. 162, comma 2-*bis* (n. 171);
- l'omessa comunicazione all'interessato, circa l'avvenuta violazione dei dati personali, da parte di fornitori di servizi di comunicazione elettronica accessibili al pubblico (cd. *data breach*) – art. 162-*ter*, comma 2 (n. 92);
- l'utilizzo illecito dei dati delle persone iscritte al Registro pubblico delle opposizioni per finalità di *marketing* – art. 162, comma 2-*quater* (n. 19);
- l'omessa o incompleta notificazione – art. 163 (n. 16);
- l'omessa adozione delle misure minime di sicurezza di cui all'art. 33 del Codice – art. 162, comma 2-*bis* (n. 15);
- la conservazione di dati di traffico telefonico e telematico per un tempo superiore a quello stabilito dall'art. 132 del Codice – art. 162-*bis* (n. 14);
- l'omessa informazione o esibizione al Garante – art. 164 (n. 14);
- l'inosservanza di un provvedimento del Garante – art. 162, comma 2-*ter* (n. 6);
- l'omessa comunicazione al Garante, circa l'avvenuta violazione dei dati personali, da parte di fornitori di servizi di comunicazione elettronica accessibili al pubblico (cd. *data breach*) – art. 162-*ter*, comma 1 (n. 2).

Un approfondimento merita il dato relativo alle 171 violazioni di cui all'art. 162, comma 2-*bis* che si è definito "trattamento illecito amministrativo". La disposizione prevede una sanzione pecuniaria, da 10.000 a 120.000 euro in relazione alla violazione delle disposizioni di cui all'art. 167. Quest'ultima disposizione, a sua volta, richiama numerose previsioni del Codice, estremamente eterogenee, e, in particolare, gli artt.: 17 (verifica preliminare), 18, 19, 20, 21, 22, commi 8 e 11 (disposi-

zioni concernenti il trattamento dei dati da parte di soggetti pubblici), 23, 25, 26, 27 (disposizioni concernenti il trattamento dei dati da parte dei soggetti privati), 45 (trasferimenti all'estero vietati), 123, 126, 129 e 130 (disposizioni specifiche per le comunicazioni elettroniche). Nel 2014 le violazioni concernenti il "trattamento illecito amministrativo" accertate hanno riguardato:

- in 101 casi, la violazione del consenso dell'interessato in rapporto agli artt. 23 e 130 del Codice;
- in 29 casi, violazioni commesse da enti pubblici (nella maggior parte dei casi comunicazioni o diffusioni di dati non sensibili senza i necessari presupposti di legge o regolamento);
- in 14 casi, violazioni delle misure e degli accorgimenti prescritti dal Garante nell'ambito di una verifica preliminare sulla base dell'art. 17 del Codice;
- in 14 casi, violazioni commesse da enti pubblici con riferimento a dati sensibili;
- in 5 casi, violazioni commesse da fornitori di reti pubbliche di comunicazione o di servizi di comunicazione elettronica con riferimento ai dati di traffico di abbonati o utenti;
- in 2 casi, violazioni commesse da soggetti privati in relazione al trattamento di dati sensibili o giudiziari;
- in 2 casi, violazioni commesse da fornitori di reti pubbliche di comunicazione o di servizi di comunicazione elettronica con riferimento all'inserimento e all'utilizzo dei dati personali relativi agli abbonati negli elenchi pubblici, cartacei o elettronici;
- in un caso, una violazione commessa in relazione al trasferimento di dati personali in Paesi extra-UE;
- in un caso, una violazione commessa da un ente pubblico con riferimento a dati giudiziari.

Analizzando i dati statistici sopra riportati si può rilevare che:

- in senso assoluto, anche per l'anno di riferimento, il maggior numero di violazioni accertate ha riguardato l'obbligo di fornire all'interessato tutte le informazioni sul trattamento dei dati, al fine di renderlo pienamente consapevole dell'effettivo utilizzo dei suoi dati personali; ciò si spiega alla luce del fatto che l'obbligo di informativa costituisce l'adempimento più generale previsto dal Codice;
- sommando le violazioni del consenso dell'interessato (n. 101) a quelle relative all'utilizzo illecito dei dati delle persone iscritte al Registro pubblico delle opposizioni per finalità di *marketing* (n. 19) si arriva ad un totale di circa 120 violazioni accertate rispetto a soggetti privati che hanno utilizzato i dati personali dei clienti senza (o contro) la volontà degli interessati. Nella gran parte dei casi queste violazioni attengono a trattamenti effettuati da aziende per finalità di *marketing* e rientrano in quel fenomeno definito *marketing* "selvaggio" in relazione al quale pervengono centinaia di segnalazioni di cittadini disturbati in particolare da chiamate indesiderate sulle proprie utenze telefoniche;
- si sono verificati i primi casi di violazioni relative all'omessa comunicazione all'interessato e al Garante, circa l'avvenuta violazione dei dati personali, da parte di fornitori di servizi di comunicazione elettronica accessibili al pubblico (cd. *data breach*); in uno dei due casi, oltre alla mancata comunicazione del *data breach* al Garante è stata anche rilevata e contestata la mancata comunicazione ai diretti interessati (92 persone) i cui dati erano stati indebitamente violati.

I procedimenti sanzionatori definiti nel 2014 con provvedimento di ordinanza ingiunzione adottato dall'Autorità, relativamente a violazioni contestate negli anni precedenti al 2014 e non definite all'epoca attraverso il pagamento spontaneo in misura ridotta da parte del contravventore, sono stati 270. Di questi, 202 hanno comportato l'applicazione di una sanzione (per un ammontare complessivo di somme ingiunte pari a 1.953.000 euro) e 68 si sono invece conclusi con l'archiviazione in quanto la parte ha potuto dimostrare nel procedimento di non aver commesso la violazione contestata o che la violazione non era ad essa imputabile.

Tra le ordinanze più rilevanti adottate si segnalano quelle relative a violazioni dell'obbligo di informativa e di acquisizione del consenso degli interessati per l'utilizzo dei dati per finalità di *marketing;* in questi provvedimenti, essendo i dati destinati a confluire all'interno di banche dati di particolare rilevanza e dimensioni, è stata applicata anche la sanzione prevista dall'art. 164-*bis*, comma 2, del Codice (ordinanza ingiunzione 8 maggio 2014, n. 231, doc. web n. 3275922; ordinanza ingiunzione 2 ottobre 2014, n. 437, doc. web n. 3747707; ordinanza ingiunzione 12 novembre 2014, n. 519, doc. web n. 3685448)

Per quanto invece riguarda i profili giuridici di maggiore interesse, si possono prendere in esame, in particolare, i seguenti casi:

- raccolte dati *online* per le quali la casella relativa al consenso al trattamento è pre-impostata per raccogliere il consenso in violazione dell'art. 23 del Codice. Per effetto di quanto previsto dall'art. 23 del Codice, il consenso al trattamento dei dati, per essere acquisito legittimamente, deve sempre essere, oltre che informato, anche libero. Relativamente a tale requisito essenziale, le manifestazioni del consenso rese obbligatorie mediante la pre-impostazione di *flag*, siano essi modificabili che non modificabili, non consentono il lecito trattamento dei dati raccolti per finalità ulteriori rispetto a quella per la quale il *form* di raccolta è preposto, così come peraltro più volte asserito dall'Autorità in diversi provvedimenti (già con provv. 10 maggio 2006, doc. web n. 1298709, e più di recente, tra gli altri, con provv. 4 luglio 2013, n. 330, doc. web n. 2542348) (ordinanze ingiunzione 18 dicembre 2014, n. 612, doc. web n. 3745935 e n. 613, doc. web n. 3750400);
- effetti della scadenza dei termini nel procedimento amministrativo con riferimento al distinto procedimento sanzionatorio dei cui alla l. n. 689/1981. Benché la l. n. 241/1990 sul procedimento amministrativo stabilisca, all'art. 2, il generale principio del dovere di rispettare il termine di conclusione del procedimento amministrativo, nessuna disposizione di legge lo ha elevato a requisito di validità dell'atto amministrativo. Pertanto, anche la violazione di un termine indicato dai Regolamenti del Garante nn. 1 e 2/2007 non vizia l'atto amministrativo (verbale di contestazione), sopravvenuto alla scadenza di un termine del procedimento cui tale atto è riferibile. Partendo da questo presupposto, la contestazione delle sanzioni amministrative accertate dal Garante in un suo provvedimento non è viziata, a condizione che sia rispettato il termine previsto dall'art. 14, l. n. 689/1981 (cfr. ordinanza ingiunzione del 12 novembre 2014, n. 520, doc. web n. 3624070);
- sanzionabilità delle telefonate promozionali effettuate oscurando il numero del chiamante. La condotta consistente nell'effettuazione di chiamate telefoniche promozionali camuffando o celando l'identità del chiamante ovvero senza fornire un idoneo recapito presso il quale l'interessato possa esercitare i diritti di cui all'art. 7 del Codice, sostanzia un illecito amministrativo riconducibile alla previsione di cui all'art. 130, comma 5, del Codice e sanzionata dall'art. 162, comma 2-*quater* in combinato disposto con gli artt. 162,

comma 2-*bis* e 167 del Codice. Ne consegue che l'invio di comunicazioni a scopo promozionale, previsto nel comma 5, si riferisce all'utilizzo di un qualsiasi mezzo, tra quelli previsti nei primi tre commi dell'art. 130, per l'effettuazione di comunicazioni promozionali, quindi anche alle chiamate con operatore (ordinanza ingiunzione 22 maggio 2014, n. 263, doc. web n. 3276281);

- autonoma valenza, quale fattispecie sanzionatoria, dell'illecito di cui all'art. 164-*bis*, comma 2, del Codice. L'Autorità, tornando ad affrontare e approfondire le tematiche relative alla sanzione sulle grandi banche dati, nel ribadire (cfr. Relazione annuale 2013) "i criteri in base ai quali le banche dati in questione possono essere definite di particolare rilevanza, indipendentemente dalla numerosità del *database*, o dimensione, in ragione della quantità di dati in esso contenuti", ha asserito, trovando poi conforto nella sentenza dell'11 marzo 2014, del Tribunale di Milano – I Sez. civ., il principio secondo cui la violazione di cui all'art. 164-*bis*, comma 2, del Codice configura una "fattispecie complessa", collegata ma autonoma rispetto a quelle presupposte. Una pluralità di violazioni commesse in relazione a banche dati di particolari dimensioni o rilevanza, determina un'offesa a un bene giuridico ulteriore rispetto a quello inciso dalle singole violazioni (che costituiscono il presupposto dell'illecito di che trattasi), in ragione del maggiore pregiudizio che si sostanzia quando i dati vengono aggregati all'interno di una banca dati con le specifiche peculiarità (banche dati di eccezionale dimensione o rilevanza) costituenti il presupposto dell'illecito in questione (ordinanze ingiunzione 8 maggio 2014, n. 231, doc. web n. 3275922; 2 ottobre 2014, n. 437, doc. web n. 3747707 e 12 novembre 2014, n. 519, doc. web n. 3685448).

Pagamenti effettuati

L'ammontare dei pagamenti effettivamente effettuati nel 2014 da parte dei soggetti nei cui confronti sono stati avviati procedimenti sanzionatori amministrativi è risultato complessivamente pari a 4.907.866 euro (cfr. sez. IV, tab. 8), di cui:

- 2.374.135 euro, pagati a titolo di definizione in via breve;
- 1.968.136 euro, a seguito di ordinanze ingiunzione adottate dal Garante in tutti i casi in cui la parte non si è avvalsa della facoltà di definizione in via breve di cui al punto precedente;
- 120.000 euro, per la definizione, in sede amministrativa, dei procedimenti relativi alla mancata adozione delle misure minime di sicurezza;
- 445.595 euro, quali ulteriori entrate derivanti dall'attività sanzionatoria (ad es., riscossione coattiva).

Gli importi relativi alle sanzioni applicate dal Garante sono versati sul bilancio dello 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 utilizzabili unicamente per l'esercizio della attività ispettiva e di divulgazione della disciplina della protezione dei dati personali.

22.6. *Le novità introdotte nel 2014 relativamente ai procedimenti sanzionatori*

Nell'ottica del continuo miglioramento delle attività procedimentali, nel 2014 sono state individuate alcune soluzioni che consentiranno di aumentare l'efficienza dell'Ufficio e, contemporaneamente, di semplificare gli adempimenti dei destinatari dei provvedimenti con riferimento al pagamento delle sanzioni amministrative. Tali profili riguardano:

- l'indicazione di un unico riferimento di conto a livello nazionale sul quale devono essere effettuati tutti i pagamenti (anziché tanti riferimenti quante sono le tesorerie provinciali, in funzione della residenza del contravventore);
- la ricezione dalla Ragioneria generale dello Stato, con cadenza mensile, di una reportistica contenente l'indicazione e tutti gli estremi dei versamenti contabilizzati sul capo X, capitolo 2373 del bilancio dello Stato ove affluiscono i pagamenti delle sanzioni in materia di protezione dei dati personali (precedentemente l'Ufficio non aveva invece alcuna evidenza di tali versamenti).

Per quanto riguarda il primo aspetto, l'aver individuato la Tesoreria provinciale di Roma quale unico ente presso cui far confluire tutti i pagamenti eviterà il dover riportare, di volta in volta, codici Iban e numeri di conto corrente postale diversi in ragione della residenza del contravventore.

Quanto al secondo aspetto, si potranno ottenere ulteriori miglioramenti:

- un maggiore controllo sui pagamenti: precedentemente il controllo dell'effettivo pagamento delle sanzioni era estremamente complesso. L'Ufficio doveva infatti basarsi sulla ricezione dei versamenti effettuati (mediante bonifici bancari o postali) e non aveva modo di verificarli se non richiedendo un riscontro all'intermediario utilizzato dalla parte per il pagamento. Con la ricezione del flusso informativo da parte della Ragioneria generale dello Stato invece si ha una rendicontazione verificata e attendibile dei versamenti effettivamente effettuati;
- una maggiore completezza e precisione nella rendicontazione dell'attività sanzionatoria: i dati sui pagamenti effettuati precedentemente avrebbero potuto essere (in parte) sottostimati, potendo sfuggire alcuni pagamenti; il sistema precedente non consentiva di disporre con precisione dei dati relativi ai versamenti effettuati dai contravventori in un dato periodo temporale. Nelle comunicazioni della Ragioneria generale dello Stato sono presenti anche i versamenti che vengono effettuati da Equitalia in ragione delle somme derivanti da ordinanze ingiunzione non pagate ed iscritte a ruolo. Tali somme, di cui precedentemente non si aveva evidenza, contribuiscono a definire l'ammontare degli incassi sul capitolo 2373 del Capo X del bilancio dello Stato. È così più agevole, alla fine dell'anno, disporre di un rendiconto puntuale di tutte le somme incassate;
- eliminazione della procedura di verifica sull'eventuale pagamento: in tutti i casi nei quali agli atti non risultava il pagamento né l'invio da parte del contravventore di memorie difensive, prima di procedere a predisporre l'ordinanza, l'Ufficio inviava una lettera tipo per verificare l'eventuale pagamento della sanzione evitando così di dover poi eventualmente revocare l'ordinanza adottata. Tale procedura non è adesso più necessaria.

Con l'invio, da parte della Ragioneria generale dello Stato, del riepilogo mensile dei versamenti effettuati (descritti precedentemente), l'Ufficio dispone adesso di dati "certificati" che rendono del tutto superfluo l'invio della contabile a dimostrazione dell'assolvimento dell'obbligo di pagamento.

Sono state pertanto modificate le istruzioni che vengono comunicate al contravventore, abolendo l'obbligo di trasmissione delle quietanze di pagamento, alleggerendo le incombenze e riducendo notevolmente i flussi documentali, specie nei casi di pagamenti rateali.

Per agevolare e orientare tutti i soggetti coinvolti nei procedimenti sanzionatori è stata infine realizzata e pubblicata sul sito una nuova sezione informativa contenente le risposte ai questi più frequenti.

22.7. *Le proposte del Garante per una revisione dell'apparato sanzionatorio del Codice e l'attualizzazione delle misure minime di sicurezza contenute nell'Allegato B al Codice*

Come anticipato (crf. par. 22.5.1), il Garante ha suggerito al Governo alcune modifiche all'attuale apparato sanzionatorio con l'invio al Presidente del Consiglio dei ministri della comunicazione denominata: "Semplificazione del quadro sanzionatorio e delle misure minime di sicurezza previste dal Codice" (nota 22 settembre 2014, doc. web n. 3531329), rinnovando l'invito anche in tempi successivi (nota 16 gennaio 2015).

Nella lettera, il Presidente dell'Autorità rappresenta che: "Le misure prospettate potrebbero assicurare significativi benefici, anche in termini economici, soprattutto alle piccole e medie imprese o comunque ai soggetti, anche pubblici, di modeste dimensioni, senza tuttavia abbassare lo *standard* delle garanzie per i cittadini e nel rispetto dei vincoli dell'Unione europea".

Il progetto di riforma del quadro giuridico in materia di protezione dei dati, infatti, si sostanzia in alcuni interventi mirati di modifica del Codice ispirati ai seguenti principi:

- semplificazione del quadro sanzionatorio e aumento dell'equità nell'applicazione delle sanzioni, mediante, fra l'altro, la ridefinizione dei confini tra le fattispecie penali e amministrative e la limitazione della responsabilità penale per la mancata adozione delle misure minime di sicurezza ai soli casi in cui ne sia derivata una conseguenza negativa nella sfera giuridica degli interessati;
- riduzione dei costi diretti e indiretti (di consulenza e assistenza legale) per i soggetti destinatari di sanzioni, mediante il ricorso diretto e automatico a modalità di estinzione agevolata dei procedimenti sanzionatori e diminuendo i casi in cui non è ammessa l'estinzione mediante oblazione;
- promozione di un aggiornamento delle misure minime di sicurezza previste dal Codice (art. 36) anche con disposizioni differenziate in ragione dei rischi effettivi per i diritti degli interessati e minimizzando l'impatto economico delle stesse, in particolare presso le piccole e medie imprese, liberi professionisti e artigiani. A tal fine, si prevede la consultazione delle categorie interessate e si affida al Garante il compito di proporre tali adempimenti sulla base dell'esperienza maturata dalla quotidiana applicazione delle relative disposizioni.

Queste modifiche appaiono ancora oggi necessarie e utili nell'ottica di bilanciare ulteriormente un assetto che, nell'esperienza quotidiana dell'Autorità, appare talvolta eccessivamente gravoso nei confronti di violazioni minori, con una ricaduta ridotta in termine di lesione effettiva dei diritti. Per altro verso, invece, l'esperienza applicativa dell'Autorità dimostra che, in ambiti nei quali gli interessi economici e la competizione sul mercato tra soggetti diversi sono molto forti, l'attuale sistema sanzionatorio risulta scarsamente dissuasivo (il caso tipico è quello del fenomeno del cd. *marketing* "selvaggio"). In questi casi si rende necessario semmai introdurre forme di progressivo automatico aggravamento delle sanzioni in caso di ripetute violazioni delle medesime disposizioni da parte dello stesso soggetto in un arco di tempo definito, al fine di disincentivare le pratiche scorrette.

Come già evidenziato al precedente par. 22.5.1, ormai indifferibile appare la revisione delle misure minime di sicurezza contenute nel disciplinare tecnico All. B al Codice, in ragione dell'obsolescenza di molte disposizioni (pensate ormai più di dieci anni fa) e del mutato contesto tecnologico di riferimento, con l'esigenza crescente di proteggere il dato non solo staticamente, allorché è memorizzato all'interno di una banca dati, ma, ancor di più, in tutte le occasioni (sempre più fre-

quenti) in cui lo stesso è oggetto di trasferimenti per mezzo delle reti di comunicazione o di accesso da parte di postazioni remote.

Tale esigenza appare ancora più evidente se si considera che, sulla base dell'attività esercitata quotidianamente dall'Autorità e di studi condotti da osservatori indipendenti, sussistono ancora carenze non trascurabili nei livelli di sicurezza garantiti dalle pubbliche amministrazioni rispetto ai dati trattati nei loro sistemi informativi. Tali carenze assumono una rilevanza ancora maggiore se si tiene presente l'accelerazione registrata negli ultimi tempi nel processo di informatizzazione della p.a., che ha determinato l'esigenza di correggere la crescente asimmetria tra la capacità d'innovazione tecnologica e gli *standard* di sicurezza adottati dalle Istituzioni.

D'altro canto, non meno rilevante appare tale esigenza in riferimento alle misure di sicurezza adottate dagli operatori privati. La collocazione non adeguata delle problematiche relative alla sicurezza dei dati personali nell'ambito delle priorità e degli investimenti operati da soggetti privati, specie se di grandi dimensioni, contribuisce alla mancata percezione degli aspetti connessi alla protezione, integrità e sicurezza dei dati quali fattori strategici di competitività, innovazione e *accountability* per le imprese, traducendosi in ultima istanza in un più generale limite allo sviluppo del Paese (con risvolti negativi, a volte, sull'intera sicurezza nazionale, come nel caso degli IXPs).

Il mancato aggiornamento delle misure minime di sicurezza contenute nel disciplinare tecnico All. B al Codice, durante questi anni, è certamente imputabile, almeno in parte, alle modalità con le quali tale procedimento di revisione deve realizzarsi ai sensi dell'art. 36 del Codice, ovvero con decreto del Ministro della giustizia di concerto con il Ministro per le innovazioni e le tecnologie e il Ministro per la semplificazione normativa.

Nel disegno di legge "Misure di semplificazione degli adempimenti per i cittadini e le imprese e di riordino normativo", attualmente all'esame del Senato (A.S. 958), è già prevista una modifica di questa norma, ma non nel senso auspicato dall'Autorità.

Considerata la particolare sensibilità e l'esperienza maturata sul campo nelle centinaia di ispezioni effettuate nei più diversi contesti tecnologici, apparirebbe più opportuno infatti affidare al Garante non solo un ruolo consultivo ma di iniziativa dell'*iter* di rinnovamento di quelle misure di minime di sicurezza la cui corretta implementazione, da parte di enti pubblici e soggetti privati, costituisce ormai una condizione necessaria ed essenziale di garanzia per i cittadini nella società dell'informazione, restituendogli anche il potere di semplificare tali misure in tutti quei contesti in cui la loro implementazione risulterebbe sproporzionata in relazione alla tutela degli interessi protetti.

23 Le relazioni comunitarie e internazionali

Nonostante le aspettative, il 2014 non ha portato, a livello europeo e internazionale, al completamento dei lavori per l'adozione dei nuovi strumenti legislativi in materia di protezione dei dati personali. Si tratta com'è noto della revisione della Convenzione n. 108/1981 del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale e delle proposte di regolamento e di direttiva che formano il pacchetto per un nuovo quadro giuridico europeo in materia di protezione dei dati.

Nel Consiglio d'Europa, il CAHDATA – comitato intergovernativo incaricato dal Comitato dei ministri di portare a termine il processo di modernizzazione della Convenzione 108, sulla base della proposta del Comitato T-PD – ha concluso il proprio mandato con l'adozione a dicembre 2014 del documento contenente la Convenzione modernizzata. Tuttavia, sul testo adottato dal CAHDATA, continuano a pesare le riserve della Commissione europea su alcuni articoli che corrispondono a nodi non ancora sciolti nell'ambito del nuovo regolamento UE (vedi par. 23.1).

In ambito UE, analogamente, sebbene sia la proposta di Regolamento generale (doc. web n. 2110215), volto a sostituire la direttiva 95/46/CE (relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali) che la proposta di direttiva sul trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e proseguimento di reati o esecuzioni di sanzioni penali (doc. web n. 2110225), volta a sostituire la Decisione quadro 977/2008 (relativa al trattamento dei dati personali trattati nell'ambito della cooperazione di polizia e giudiziaria in materia penale), siano state adottate in prima lettura, con emendamenti, dal Parlamento europeo, non sono stati portati a termine i lavori presso il Consiglio UE che deve ancora addivenire ad una propria posizione comune (v., in proposito, par. 23.1).

In sede OCSE, è proseguito il lavoro di revisione delle Linee guida sicurezza dell'OCSE del 2002 *(Recommendation Concerning Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security)* che andranno ad affiancare le nuove Linee guida *privacy* dell'OCSE, adottate nel 2013 (cfr. Relazione 2013, p. 189).

Il Garante ha continuato ad impegnarsi per poter contribuire attivamente a tali processi di riforma partecipando ai diversi gruppi e comitati di lavoro istituiti, in particolare attraverso gli sforzi profusi nel semestre di Presidenza italiana dell'UE per cercare di far progredire i lavori sui testi in discussione presso il Consiglio (per una versione d'insieme v. sez. IV, tab. 25).

Il 2014 si è caratterizzato invece per l'intensificarsi delle attività di cooperazione – tema al centro dei lavori della Conferenza di primavera dei Garanti europei – tra le autorità di protezione dei dati europee (soprattutto con riferimento ai trattamenti di dati effettuati dalle multinazionali che operano *online*) e anche a livello internazionale (cfr. par. 23.2).

Contributi importanti per chiarire il quadro applicativo della disciplina in materia di protezione dei dati sono inoltre pervenuti dalla Corte di giustizia che si è espressa con importanti sentenze sulla nozione di stabilimento e sul diritto alla deindicizzazione dai motori di ricerca (cfr. par. 23.3, doc. web n. 3127044), sull'indi-

pendenza delle autorità di protezione dei dati (doc. web n. 3845166), sulla direttiva che imponeva l'obbligo di conservazione dei dati di traffico telefonico e telematico per finalità di polizia (cd. *data retention*) (doc. web n. 3043705: cfr. par. 23.3) e sulla definizione del concetto di trattamento di dati per finalità strettamente personali (doc. web n. 3845146: cfr. par. 14.5,).

Il tema della sorveglianza ha continuato ad essere al centro della riflessione delle autorità di protezione dei dati. In particolare, le autorità europee di protezione dei dati – riunite nel Gruppo Art. 29, del quale nel 2014 il presidente Antonello Soro è stato eletto vice-presidente – hanno adottato una dichiarazione comune volta a riaffermare i valori condivisi a livello europeo e a proporre alcune azioni concrete al fine di sviluppare un quadro di principi per una *governance* europea democratica e rispettosa dei diritti fondamentali. La dichiarazione, presentata in occasione del *European data governance forum* tenutosi a Parigi l'8 dicembre 2014 (v. par. 23.2), richiama la responsabilità di tutti i soggetti, privati e pubblici, affinché sia assicurato il rispetto di tali principi, specie nella raccolta ed utilizzo dei dati personali nell'economia digitale.

23.1. *La riforma del quadro giuridico europeo in materia di protezione dei dati*

Dopo che, il 12 marzo 2014, il Parlamento europeo ha votato la propria posizione in prima lettura, la pressione affinché il Consiglio UE terminasse l'analisi del "pacchetto" protezione dati si è fatta indubbiamente più forte. Colloqui interistituzionali necessari a mettere a punto un testo di compromesso (attraverso il cd. "trilogo" fra Parlamento, Commissione e Consiglio UE) potranno infatti iniziare soltanto quando il Consiglio avrà raggiunto, su entrambe le proposte legislative, un accordo sulla propria posizione negoziale. La Presidenza greca e, quindi, quella italiana hanno dato un forte impulso ai lavori del competente gruppo di lavoro (DAPIX) giungendo, per quanto riguarda in particolare la proposta di regolamento, ad un cd. "accordo generale parziale" su alcuni elementi importanti: art. 1 (Oggetto e obiettivi); art. 3 (Campo di applicazione territoriale); art. 4, limitatamente alla definizione di "stabilimento principale" e di "*Binding corporate rules*"; art. 6 (Liceità del trattamento); art. 21 (Limitazioni alle disposizioni del Regolamento); capo IV (Obblighi dei titolari e responsabili di trattamento, artt. 22-39-*bis*); capo V (Trasferimenti internazionali di dati, artt. 40-45); capo IX (artt. 80-85 - Disposizioni relative a particolari tipologie di trattamento: per finalità giornalistiche, esercizio libertà di espressione, accesso a documenti pubblici, contesto lavorativo, archivi, trattamenti scientifici, statistici, storici, norme in materia di riservatezza professionale, confessioni religiose). È stato, inoltre, ottenuto dai Ministri UE durante il Consiglio GAI di dicembre 2014 un sostanziale *endorsement* per l'architettura generale del meccanismo di "sportello unico" (*One-Stop-Shop*, capi VI e VII: artt. 46-72), così come rielaborato dalla Presidenza italiana (v. *infra*).

Il Garante ha partecipato costantemente alle riunioni del DAPIX ed ha intensificato la propria collaborazione, in particolare con la Presidenza italiana del secondo semestre del 2014, fornendo proprie analisi e formulando osservazioni e proposte anche alla luce dei pareri e dei documenti adottati in materia dal Gruppo Art. 29 (v. Relazione 2013).

Guardando agli elementi oggetto di accordo per quanto concerne la proposta di regolamento, vale la pena di sottolineare, in particolare, gli ulteriori margini di flessibilità introdotti per gli Stati membri attraverso l'art. 1. In base al testo modificato sotto la Presidenza italiana, essi saranno autorizzati a "introdurre o mantenere"

disposizioni che specifichino ulteriormente quelle contenute nel regolamento per i trattamenti svolti "nel pubblico interesse", in aggiunta alle disposizioni di deroga (già previste dagli artt. 6 e 21, e modellate su quelle contenute anche nell'attuale direttiva 95/46/CE, soprattutto dall'art. 13 di quest'ultima). Numerosi Stati membri hanno, infatti, chiesto di poter disporre di un maggiore margine di "flessibilità", indipendentemente dalla natura pubblica o privata del titolare di trattamento, per consentire soluzioni anche più stringenti rispetto ai requisiti del regolamento, nel presupposto di un pubblico interesse da perseguire (quest'ultimo definito in modo più specifico attraverso un apposito "considerando").

Importante anche l'accordo sul tema (orizzontale) del cd. approccio basato sul rischio del trattamento, tale da calibrare gli obblighi del titolare sul rischio che ciascun trattamento comporta, e che si inquadra nel contesto più ampio del principio di *accountability* (responsabilizzazione dei titolari di trattamento). Il testo approvato dai ministri durante il Consiglio GAI di ottobre 2014 individua il livello di rischio su cui ponderare gli obblighi dei titolari (rischio "elevato"), definendo (in via generale) i fattori da tenere in considerazione (art. 22) e quindi declinando l'approccio "basato sul rischio" in varie disposizioni (artt. 23, 26, 28, 30, 31, 33 e 34); queste ultime mirano essenzialmente a fornire indicazioni su natura, contesto, campo di applicazione, scopi dell'attività di trattamento dei dati e sui rischi esistenti per i diritti e le libertà degli interessati. Ad esempio, il trattamento di dati pseudonimizzati (che restano dati personali, come precisato in un apposito considerando) viene ritenuto utile a ridurre il rischio del trattamento, mentre l'obbligo di notifica all'autorità di controllo delle violazioni relative ai dati personali, esteso dalla proposta di regolamento a tutti i titolari di trattamento (artt. 31 e 32), è stato riformulato in chiave di rischio per evitare eccessivi oneri amministrativi e, per altro verso, un eccesso di notifiche per violazioni alle Autorità garanti. Rientrano in quest'ambito anche la valutazione di impatto (obbligatoria) e la consultazione preventiva dell'autorità di controllo (artt. 33 e 34), per cui si prevede l'obbligo per i titolari di consultare l'autorità solo nei casi in cui l'esito della valutazione di impatto si concluda con il riconoscimento di un rischio "elevato" nonostante le misure di mitigazione del rischio adottate dal titolare; fra queste ultime si ricordano, in particolare, la nomina di un DPO (*Data Protection Officer*, o "incaricato della protezione dati") (artt. 35-37), che il documento propone come facoltativa in via generale, l'adozione (e l'osservanza) di specifici codici deontologici settoriali, anche europei (art. 38 e 38-*bis*), il rilascio di certificazioni anche su base europea (art. 39 e 39-*bis*), con intervento delle autorità di protezione dati al fine di "certificare i certificatori". A tale proposito, il Gruppo Art. 29 aveva sottolineato (in uno "*Statement*" pubblicato sul punto nel mese di maggio 2014, WP 218, doc. web n. 3815164) la necessità di interpretare il concetto di "rischio" guardando all'intero impatto che il trattamento di dati personali può determinare sugli interessati (quindi anche sulla loro dignità), andando al di là del semplice "danno" o "nocumento", ed alla luce di fattori quanto più oggettivi possibili. Il Gruppo ha altresì rappresentato che la modulazione degli obblighi dei titolari in base al rischio non può mai comportare l'eliminazione assoluta di tali obblighi e che i diritti degli interessati non possono essere compressi per motivi legati al rischio "trascurabile" del trattamento, invocando il coinvolgimento delle autorità di controllo qualora l'analisi del rischio indichi un parametro elevato nonostante le misure di mitigazione adottate.

Per quanto riguarda i trasferimenti di dati personali verso Paesi terzi (capo V), il testo concordato durante la Presidenza greca (giugno 2014) mantiene l'impostazione della proposta della Commissione, che prevede un sistema gerarchico non dissimile da quello dell'attuale direttiva (adeguatezza del Paese terzo; in caso di non-adegua-