rezza (5), mancato adempimento di una deliberazione del Garante (1), trattamento illecito dei dati (1), falsità nelle dichiarazioni e notificazioni al Garante (3) e altre fattispecie (2).

Ventisei sono stati i procedimenti connessi al *cd. "ravvedimento operoso"* in materia di misure minime di sicurezza, previsto dall'art. 169, comma 2, del Codice.

Tale disposizione prevede, come noto, che nel caso in cui venga rilevata una violazione di una o più delle misure minime di sicurezza specificatamente previste dal Disciplinare tecnico sulle misure minime di sicurezza (Allegato B. al Codice) il Garante, a seguito di una prescrizione da impartirsi alla persona individuata come responsabile della predetta violazione, verificato il ripristino delle misure violate, possa ammettere i destinatari della prescrizione al pagamento pari a 1/4 del massimo della sanzione prevista corrispondenti a 12.500 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.

L'attività di cui sopra ha riguardato venti persone (in qualità di titolari/responsabili dei trattamenti), per un totale di sanzioni applicate pari a 335.329 euro.

19.4.2. Sanzioni amministrative

In conseguenza delle ispezioni effettuate, sono stati avviati trecentotrentotto procedimenti sanzionatori amministrativi (di cui centocinquantacinque ad opera del Dipartimento e centottantatre da parte della Guardia di finanza e altri organi accertatori).

Come evidenziano i dati di seguito riportati, anche per quanto attiene l'attività sanzionatoria, nell'anno 2008, si è registrato un notevole incremento.

Anno	2002	2003	2004	2005	2006	2007	2008
Violazioni contestate	46	27	27	94	158	228	338

Le sanzioni amministrative contestate, per un totale compreso tra un minimo di 1.113.000 e un massimo di 6.678.000 euro, hanno riguardato:

- omessa o inidonea informativa (311);

- omessa notificazione (12);

- omessa risposta alle richieste del Garante (15).

A fronte delle contestazioni notificate sono stati riscossi 1.061.843 euro a titolo di definizione in via breve.

L'incidenza delle violazioni, sia penali che amministrative, riscontrate è stato pari a circa al 67% sul totale delle ispezioni.

L'adempimento più sanzionato è quello relativo alla 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.

Occorre evidenziare che tale violazione assume particolare rilevanza nei casi in cui la legge impone al titolare del trattamento di acquisire anche il consenso dell'interessato per specifiche finalità (*ad es.*, per l'utilizzo dei dati per finalità di *marketing*, o per la comunicazione di dati a terzi). In questi casi, l'omessa o inidonea informativa produce effetti anche sulla validità del consenso eventualmente acquisito che, sulla base di quanto previsto dall'art. 23, comma 3, del Codice, può ritenersi valido solo se sono state fornite all'interessato le informazioni di cui all'art. 13 del Codice.

Delle contestazioni effettuate per l'omessa o inidonea informativa, circa il 32% sono da riferirsi a segnalazioni relative a trattamenti effettuati, attraverso *call center*, da compagnie telefoniche in relazione all'attivazione di servizi non richiesti, a riprova dello straordinario sforzo compiuto nel 2008 dall'Autorità per contrastare tale fenomeno.

19.4.3. Il nuovo apparato sanzionatorio

Il decreto-legge n. 207/2008, convertito nella legge 27 febbraio 2009, n. 41, ha apportato significative modifiche all'apparato sanzionatorio del Codice. Le modifiche si sono concentrate, in massima parte, sulle sanzioni amministrative mentre è rimasto sostanzialmente inalterato l'impianto sanzionatorio penale.

In linea generale, gli interventi hanno comportato: un aumento delle pene pecuniarie previste per ciascuna violazione; la previsione di nuove ipotesi sanzionatorie; la creazione di meccanismi per consentire una maggiore modulabilità della sanzione in rapporto al

caso concreto in ragione della minore o maggiore gravità, della circostanza che le violazioni siano state commesse in relazione a banche di dati di particolare rilevanza o dimensioni, del coinvolgimento di un maggior numero di interessati e delle condizioni economiche del contravventore.

Fra le nuove fattispecie sanzionatorie amministrative sono state previste, all'art. 162, comma 2-*bis*, le ipotesi di trattamento illecito e di omissioni nell'adozione delle misure minime di sicurezza (già sanzionate penalmente dagli artt. 167 e 169 del Codice, articoli tuttora vigenti).

La sanzione amministrativa (da 20.000 euro a 120.000 euro) potrà essere contestata in tutti i casi di violazione delle disposizioni richiamate dall'art. 167 nonché nei casi di violazione delle misure minime di sicurezza previste dal Codice e, per quanto riguarda le misure minime di sicurezza, senza la possibilità di avvalersi dell'estinzione del procedimento sanzionatorio con il pagamento in misura ridotta.

È stata inoltre introdotta, all'art. 162, comma 2-*ter*, una specifica fattispecie sanzionatoria amministrativa (da 30.000 euro a 180.000 euro) nei casi di inottemperanza ai provvedimenti del Garante che prescrivono, anche d'ufficio, ai titolari del trattamento le misure necessarie o opportune al fine di rendere il trattamento conforme alle disposizioni vigenti o che prevedono il blocco o il divieto del trattamento.

La norma rafforza la cogenza delle determinazioni dell'Autorità, fino ad oggi garantita, limitatamente alla violazione dei provvedimenti di blocco e di divieto del trattamento nonché di quelli relativi alla decisione dei ricorsi, dalla sanzione penale prevista dall'art. 170 del Codice.

Per quanto riguarda i meccanismi introdotti al fine di modulare le sanzioni amministrative, va evidenziato in primo luogo che l'art. 164-*bis*, comma 1, prevede la possibilità di contestare le sanzioni accertate applicando una riduzione a due quinti dei limiti minimo e massimo previsto per ciascuna violazione, nei casi di minore gravità della violazione stessa o in relazione alla natura economica e sociale dell'attività svolta dal contravventore.

Di contro, i commi 2 e 3 del medesimo articolo prevedono delle particolari *"aggravanti"* che determinano un sensibile aumento delle sanzioni:

- in caso di più violazioni di un'unica o di più disposizioni commesse, anche in tempi diversi, in relazione a banche di dati di particolare rilevanza o dimensioni (sanzione da 50.000 euro a 300.000 euro senza la possibilità di avvalersi dell'estinzione del procedimento sanzionatorio con il pagamento in misura ridotta);
- in altri casi di maggiore gravità e, in particolare, di maggiore rilevanza del pregiudizio per uno o più interessati, ovvero quando la violazione coinvolge numerosi interessati, con aumento dei limiti minimo e massimo delle sanzioni previste per ciascuna violazione in misura pari al doppio.

Tutte le sanzioni possono essere, inoltre, ai sensi dell'art. 164-*bis*, comma 4, aumentate fino al quadruplo quando possono risultare inefficaci in ragione delle condizioni economiche del contravventore.

20. Le relazioni internazionali

La mancata entrata in vigore del Trattato di Lisbona ha rallentato i progetti delle autorità di protezione dei dati personali europee, riunite nel Gruppo art. 29 e nel Gruppo di lavoro Polizia e Giustizia, di valutare l'impatto delle nuove previsioni in materia di protezione dei dati personali. Il Trattato infatti richiama espressamente ed ingloba nel quadro giuridico le disposizioni della *"Carta dei diritti fondamentali"*, che, com'è noto, all'art. 8 ha introdotto il diritto fondamentale delle persone alla tutela dei dati personali, affiancandolo all'art. 7 che riguarda il diritto alla riservatezza. Sempre il Trattato, nel prevedere la fine della divisione in pilastri dell'ordinamento comunitario, chiede un quadro di riferimento tendenzialmente unico in materia di trattamento dei dati personali. Giova ricordare che oggi nell'ambito del *cd. "primo pilastro"* – che riguarda i settori coperti dal diritto comunitario – esiste un quadro armonizzato di princìpi che, nel garantire la libera circolazione dei dati personali tra i Paesi dell'Unione europea, assicura agli individui un elevato livello di tutela, costituito dalla Direttiva 95/46/Ce sulla tutela delle persone rispetto al trattamento di dati personali e sulla libera circolazione di tali dati e dalla 2002/58/Ce che specifica i princìpi della direttiva generale in relazione al trattamento dei dati personali nell'ambito delle comunicazioni elettroniche. Nessun principio esiste al momento per quanto riguarda i trattamenti di dati che si svolgono nel *cd. "secondo pilastro"* (politica estera e di sicurezza comune), mentre è recentemente stata adottata una decisione quadro sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale che dovrà essere attuata dai Paesi dell'Unione entro la fine di novembre 2010. L'attenzione delle Autorità si è comunque mantenuta sul quadro giuridico generale per valutarne la tenuta e migliorarne l'attuazione, ovvero intervenire sulle modifiche proposte, ad esempio alla direttiva sulla *privacy* nelle comunicazioni elettroniche, o al nuovo programma di lavoro in materia di polizia e sicurezza, che sostituirà il *cd. "Programma de L'Aja"*.

Il Garante ha attivamente partecipato a diversi gruppi di lavoro cooperando con le autorità europee e mondiali di protezione dei dati personali (*v. par.* 20.1 e seguenti). In alcuni casi ha anche svolto, come per il Gruppo di lavoro polizia e giustizia, un determinante e propositivo ruolo di iniziativa.

Da segnalare che il cons. Giovanni Buttarelli, che ha svolto il ruolo di segretario generale dal momento dell'istituzione dell'Autorità, nel dicembre 2008 è stato nominato Garante europeo aggiunto dei dati personali.

Occorre evidenziare gli importanti contatti intercorsi tra il Garante e il Parlamento europeo, nonché con il Commissario per i diritti umani del Consiglio d'Europa in particolare in relazione alle iniziative del Governo italiano per utilizzare i poteri di emergenza di protezione civile in alcune aree metropolitane (Napoli, Roma, Milano) in cui vivono popolazioni nomadi. L'annuncio del censimento rom ha destato preoccupazioni forti in tutta Europa e la Commissione europea è intervenuta richiedendo non solo al Governo, ma anche al Garante, di indicare l'impatto di tali iniziative sui diritti fondamentali ed in particolare sul diritto alla protezione dei dati personali. Il Parlamento europeo, dopo aver adottato una risoluzione critica nel luglio 2008 ha inviato componenti della Commissione Libe, per incontri con le autorità. Il Garante ha nell'occasione descritto al Comitato le azioni svolte per accertare il tipo di trattamento di dati e, successivamente, per definire le modalità idonee ad assicurare il rispetto dei princìpi di protezione dei dati.

Il Garante, infatti, anche sulla base di notizie di stampa circa l'eventuale ricorso a forme di rilevazione anche biometriche (impronte digitali) estese ai minori, per finalità di identificazione o di censimento di comunità di nomadi, ha chiesto informazioni, in particolare ai Prefetti di Roma, Milano e Napoli, rilevando tra l'altro che l'adozione di tali misure potrebbe determinare l'insorgere di delicati problemi discriminatori, potenzialmente lesivi della dignità delle persone e specialmente dei minori.

Al riguardo, il Ministero dell'interno ha informato l'Autorità dell'intenzione di promuovere l'adozione di alcune linee-guida rivolte ai prefetti in merito alla raccolta dei dati relativi al censimento delle comunità nomadi.

Con il *provvedimento* del 17 luglio 2008 [doc. *web* n. 1537659] l'Autorità ha quindi espresso il proprio parere favorevole sullo schema di linee-guida messe a punto dal Ministero dell'interno per l'attuazione delle ordinanze adottate dal Presidente del Consiglio dei ministri il 30 maggio 2008 concernenti insediamenti di comunità nomadi nelle regioni Campania, Lazio e Lombardia. Le linee-guida stabiliscono i princìpi fonda-

mentali e le modalità da seguire nell'identificazione di chi risiede nei campi nomadi e tengono conto delle indicazioni e delle raccomandazioni in precedenza formulate dall'Autorità.

Anche l'incontro con il Commissario Hammarberg ha avuto come oggetto l'iniziativa del Governo italiano ed il ruolo svolto dal Garante.

L'Ufficio ha anche seguito con particolare attenzione le attività dei ministeri degli affari esteri e dell'interno sia per definire ed attuare le misure necessarie per l'emissione dei passaporti elettronici ed integrare nel *chip* le impronte digitali del titolare, come prescritto dai regolamenti comunitari, sia per la costruzione della parte nazionale del sistema Vis (sistema informativo visti) e la preparazione degli uffici consolari alle relative procedure.

Ha inoltre posto in essere le azioni necessarie per gli accertamenti preliminari sulla legittimità dei trattamenti svolti nella parte nazionale dei sistemi europei di informazione, partecipando alle decisioni adottate dalle Autorità di controllo Europol, Schengen, Eurodac ed alle azioni di *enforcement* avviate dal Gruppo art. 29.

Conferenze delle autorità su scala internazionale

La 30ma Conferenza internazionale delle autorità di protezione dati si è tenuta a Strasburgo dal 15 al 17 ottobre, organizzata congiuntamente dall'Autorità francese per la protezione dei dati (Cnil) e dall'Autorità federale tedesca (Bfd), per celebrare il trentennale dell'istituzione dei due organismi. La partecipazione è stata consistente, con oltre cinquecento iscritti provenienti da sessanta Paesi che si sono confrontati su tematiche legate da un unico filo conduttore: "*come tutelare la privacy in un mondo che non conosce più frontiere*".

Le prime due giornate, articolate in sei sessioni, hanno affrontato temi assai diversi quali l'equilibrio fra *privacy* e sicurezza, le opportunità di trasformare la tutela della *privacy* in un bene primario anche per le imprese, i rischi legati alle *social network*, le debolezze e i punti di forza dell'attuale quadro normativo regionale ed internazionale. La terza giornata è stata riservata, come è prassi, alla discussione fra le sole autorità di protezione dei dati e all'adozione di documenti e risoluzioni.

Fra queste ultime ricordiamo, in particolare, la Risoluzione sulla *privacy on-line* dei minori e la Risoluzione sull'urgenza di tutelare la *privacy* in un mondo senza frontiere. La prima sottolinea la necessità di educare e sensibilizzare alla protezione dei dati personali

ed invita *provider* e operatori in genere, ad applicare il principio di minimizzazione nel trattamento di dati relativi a minori. La seconda mira alla creazione di un gruppo di lavoro, comprendente anche l'Autorità italiana e coordinato dall'Autorità nazionale spagnola, per definire *standard* internazionali in materia di *privacy* sulla base dei princìpi già definiti in altri strumenti di varie regioni del mondo – in particolare la Convenzione 108/1981 del Consiglio d'Europa ed i princìpi Ocse ed Apec.

Ancora va menzionata la Risoluzione sulla costituzione di un Comitato che rappresenti la conferenza in occasione di incontri internazionali, che prevede la creazione di un Comitato ristretto (comprendente anche l'Autorità italiana) per far ottenere alla Conferenza lo *status* di *"osservatore"* presso vari organismi internazionali quali Ocse, Iso, Apec, Itu, Unesco.

Infine, la Risoluzione sulla tutela della *privacy* nei servizi di *social network*, all'interno della quale, anche alla luce del cosiddetto *"Memorandum di Roma"*, adottato dal Gruppo di Berlino durante l'incontro ospitato a Roma nel mese di marzo 2008 (*v. Relazione* 2007 *p.* 173), si invitano gli utenti a valutare con attenzione se e cosa pubblicare in rete, e si ricorda ai fornitori di tali servizi l'obbligo di informare adeguatamente gli utenti sulla natura dei trattamenti effettuati in rete e sui rischi possibili. Inoltre, la Risoluzione suggerisce l'applicazione di idonee misure (anche tecniche) per evitare che i dati personali siano estratti dai profili contenuti all'interno di siti di *social network* senza il consenso degli utenti (*ad es.*, attraverso gli algoritmi dei motori di ricerca esterni). La Risoluzione, infine, contiene ulteriori raccomandazioni che riguardano, in particolare, la necessità di consentire agli utenti di limitare la visibilità dell'intero profilo e di recedere facilmente dal servizio cancellando ogni informazione pubblicata sul *social network*; cautele ancora maggiori devono essere messe in atto qualora l'utente (come spesso avviene in questi casi) sia un minore.

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

Il Gruppo art. 29 (che riunisce i rappresentanti delle autorità europee in materia di protezione dei dati personali, ed è stato istituito ai sensi dell'art. 29 della Direttiva 95/46/Ce),

ha proseguito l'attuazione del programma biennale di attività adottato nel 2007 (*cfr. Relazione* 2007, *p.* 160).

In particolare, con riferimento al miglioramento dell'applicazione della Direttiva 95/46/Ce, sono stati previsti interventi volti a chiarire l'interpretazione di alcuni aspetti chiave, primi tra tutti la nozione di "*data controller*" e quella di "*data processor*". L'analisi, approfondita nell'ambito di uno specifico gruppo di lavoro, si è posta l'obiettivo di meglio definire la portata applicativa delle nozioni di *"titolare"* e di *"responsabile"* del trattamento, in particolare in vista dell'allocazione della relativa responsabilità, dell'individuazione dei rispettivi ruoli in caso di *outsourcing*, nonché delle ipotesi di contitolarità del trattamento.

In ordine alla protezione dei dati nell'ambito dei trasferimenti internazionali, particolare rilevanza è stata attribuita all'analisi di strumenti quali le *binding corporate rules* e l'accordo *Safe Harbor*. In questo contesto, si sono inserite le attività di approfondimento e di riflessione volte alla delineazione di linee-guida per le imprese e alla modifica della procedura di cooperazione in materia di *Bcr* (*v.* prosieguo), nonché le valutazioni relative all'implementazione dell'accordo *Safe Harbor*, intensificatesi in occasione del *Workshop on international transfers of personal data* (Bruxelles, 21.10.08). Parimenti, è stato confermato l'impegno del Gruppo ad esprimersi, come richiesto dalla Commissione, in merito alla valutazione di adeguatezza di Israele, Andorra, Nuova Zelanda ed Ecuador.

In materia di nuove tecnologie, diversi sono gli obiettivi rilanciati dai Garanti europei; in particolare, si ricorda l'impegno a completare il lavoro già intrapreso con riferimento ai motori di ricerca e ai *social network*; quello di giungere a una seconda opinione sulla direttiva *e-privacy*; quello di proseguire le riflessioni in materia di *Rfid* e di profilazione.

Tra gli impegni assunti, si collocano anche alcuni di carattere interno, relativi al miglioramento dell'efficacia dell'attività con azioni volte, in particolare, all'instaurazione di buone pratiche di lavoro, al perfezionamento della comunicazione tra le autorità, all'implementazione del regolamento sulle procedure interne di funzionamento dei sottogruppi (*cfr.* WP 157).

Infine, tra le priorità del programma di lavoro, sono state inserite le tematiche relative

a dati sanitari e trattamenti per finalità epidemiologiche, "*pre-trial discovery*", protezione dei dati e minori, "*credit histories*".

Per migliorare ed affinare le verifiche interne della corretta applicazione dei princìpi di protezione dei dati, è stato inserito nel programma di attività l'avvio di una nuova azione comune di verifica nel settore della conservazione dei dati di traffico telefonico e telematico, scelto in connessione con l'entrata in vigore della *cd. "direttiva Frattini"* 2006/24/Ce.

Diversi sono stati i documenti adottati dal Gruppo art. 29: di seguito si segnalano i principali.

Parere 3/2008 sugli *standard* Wada in materia di *anti-doping*

Il Gruppo art. 29 ha espresso un parere sul progetto di *standard* internazionale elaborato dall'Agenzia mondiale *anti-doping* (*World Anti-Doping Agency*-Wada), volto a fissare le regole in materia di protezione dei dati trattati da organizzazioni e soggetti che operano nel settore dell'*anti-doping* sportivo (*cfr.* WP 156).

Il Gruppo ha accolto con favore l'iniziativa della Wada anche alla luce dell'estensione geografica (globale) della sua applicazione. Tuttavia, non ha sostenuto interamente le previsioni degli *Standard*, considerata la presenza al loro interno di non poche lacune rispetto al livello minimo di tutela richiesto dalla normativa europea in materia di protezione dei dati.

Particolari raccomandazioni sono state suggerite con riguardo alle definizioni, ai princìpi di necessità e di proporzionalità, al trattamento dei dati sensibili, al consenso dell'interessato, all'informativa, alle attività di comunicazione e di conservazione dei dati e all'esercizio dei diritti da parte degli interessati.

Inoltre, particolare attenzione è stata dedicata all'implementazione della banca dati Adams, con sede in Canada, nella quale dovrebbero confluire ed essere conservati i dati che gli atleti sono tenuti a comunicare alle diverse organizzazioni *anti-doping*.

Sempre nell'ambito del progetto di *standard* internazionale per la protezione dei dati personali, il Gruppo art. 29 ha istituito un sottogruppo, per approfondire gli aspetti maggiormente problematici ed elaborare un secondo parere in materia.

Tra tali questioni si sono in particolare segnalate: il funzionamento del *database* Adams; l'individuazione della base giuridica del trattamento; le modalità del trattamento di dati

sensibili e le tipologie dei dati trattati; la pubblicazione in Internet delle decisioni in materia di *anti-doping*; il trasferimento dei dati; la tipologia delle informazioni richieste agli atleti da inserire nel *cd. "modulo whereabouts"* volto a consentire la reperibilità degli atleti ai fini di controlli *anti-doping*; l'individuazione del titolare del trattamento; l'informativa da prestare agli interessati (*v. par.* 20.3)

Parere sulla ricerca di *"pre-trial discovery"*

Il Gruppo dei Garanti europei ha adottato un documento di lavoro (*cfr.* WP 158) volto a delineare le linee-guida in materia di trattamento di dati personali nell'ambito delle richieste di informazioni, provenienti per lo più dagli Stati uniti, relative alle attività di *"pre-trial discovery"* (ovvero le attività di ricerca della prova connesse all'instaurazione di un procedimento giudiziario).

Tale intervento è stato reso necessario dal crescente aumento delle attività di trasferimento transfrontaliero di dati personali collegato all'attuazione di ordini di trasmissione o di esibizione dei documenti emanati da giudici statunitensi.

La questione ha coinvolto in particolare società, spesso sussidiarie o controllate di gruppi multinazionali aventi sede legale negli Stati uniti, cui è stato richiesto, dalla capogruppo, di fornire informazioni (comprensive anche di dati personali relativi a dipendenti, clienti o fornitori) considerate rilevanti nell'ambito delle investigazioni difensive o delle attività pre-contenziose di ricerca della prova connesse all'instaurazione di un procedimento giudiziario. Il recente aumento di richieste di tal tipo, che, tra l'altro, comportano un trasferimento di dati personali, anche sensibili, verso paesi che non offrono adeguate garanzie di protezione, ha evidenziato la presenza di non poche problematiche in considerazione dell'applicazione della disciplina prevista dalla 95/46/Ce.

I Garanti europei hanno, dunque, rappresentato l'esigenza di contemperare le esigenze difensive, come disciplinate dalla normativa statunitense in materia di *"pre-trial discovery"*, con i princìpi europei di protezione dei dati personali sanciti dalla Direttiva 95/46/Ce.

Sono state così emanate alcune linee-guida, indirizzate ai titolari del trattamento stabiliti in uno Stato membro, volte a ribadire che alle richieste di informazioni connesse ad esigenze difensive nell'ambito di procedimenti civili si applicano le norme in materia di protezione dei dati personali (il documento non si riferisce al processo penale).

Il testo (*cfr.* WP 158) dedica particolare attenzione alle finalità del trattamento, individuate con riferimento all'utilizzo delle informazioni così raccolte (conservazione, comunicazione, successivi trasferimenti o usi ulteriori), soprattutto in vista dell'applicazione dei princìpi di proporzionalità e di stretta finalità del trattamento, nonché delle previsioni della direttiva in materia di conservazione dei dati.

Speciale rilevanza è, inoltre, riservata alla determinazione della base giuridica del trattamento, la quale può essere alternativamente individuata, a seguito di un'analisi effettuata caso per caso, nel consenso dell'interessato (purché sia possibile dimostrarne la manifestazione libera e informata), nell'adempimento di un obbligo di legge (nei soli casi in cui all'interno dello Stato membro, in cui i dati sono raccolti, viga un obbligo normativo di conformarsi ad un ordine giudiziario proveniente da un giudice straniero), nel perseguimento di un legittimo interesse del titolare o di un terzo a condizione che non siano pregiudicati i diritti e le libertà fondamentali dell'interessato (operando una valutazione che tenga conto della effettiva rilevanza dell'informazione personale rispetto alle esigenze di difesa in giudizio).

Inoltre, il documento ribadisce i princìpi in materia di modalità del trattamento (art. 6 della Direttiva 95/46/Ce), di rilascio di una preventiva informativa agli interessati, in particolare tenendo conto della circostanza che i dati, nella maggior parte delle ipotesi, non sono raccolti presso l'interessato (artt. 10-11 della Direttiva 95/46/Ce), di esercizio dei diritti (artt. 12-15 della direttiva) e di adozione di adeguate misure di sicurezza (art. 17).

Infine, un'attenta riflessione è stata condotta con riferimento all'applicazione degli artt. 25-26 della direttiva in materia di trasferimenti transfrontalieri di dati personali. In tale contesto, il Gruppo dei Garanti europei ha incoraggiato l'adesione all'accordo *Safe Harbor*, nonché l'adozione di *standard contractual clauses* o di *binding corporate rules*, precisando però la necessità che il trasferimento di tali dati per finalità di difesa in giudizio sia espressamente ricompreso tra quelli coperti dagli strumenti sopracitati. La deroga di cui all'art. 26 (1), lett. *d*), della direttiva ("tr*asferimento per finalità di esercizio di un diritto in giudizio*") non può, infatti, costituire una base giuridica sufficiente a legitti-

mare trasferimenti *"in massa"* di dati personali verso paesi che potrebbero non assicurare una tutela adeguata.

Le *Binding corporate rules*

Particolarmente intensa è stata l'attività del Gruppo dei Garanti europei in materia di *"Binding corporate rules (Bcr)"*.

Tale strumento, che trae la propria efficacia giuridica dal rilascio di specifiche autorizzazioni nazionali al trasferimento dei dati personali verso Paesi terzi, ha richiesto un'attenta riflessione volta a chiarirne la natura giuridica e a meglio definirne le modalità di applicazione.

Il lavoro del Gruppo art. 29 è stato, in particolare, dedicato all'analisi dello strumento delle *Bcr* e alla sua effettiva diffusione nell'ambito dei grandi gruppi multinazionali d'impresa. In questo contesto è stata valutata l'opportunità di rilanciarne l'efficacia, semplificare gli oneri connessi al loro utilizzo e rendere una maggiore trasparenza con riferimento alle relative procedure di adozione.

Sono state così predisposte alcune linee-guida esemplificative per le società, comprensive di una *check list* contenente tutti gli elementi necessari alla redazione delle *Bcr* da parte degli organismi coinvolti (*cfr.* WP 153); la redazione di specifiche Faq volte a chiarire caratteristiche e contenuto delle *Bcr* medesime (*cfr.* WP 155); l'individuazione di un *"modello"* esemplificativo di *Bcr*, in grado di costituire una guida utile per le società interessate (*cfr.* WP 154).

Parimenti, è stato intrapreso un lavoro di approfondimento e di semplificazione della procedura amministrativa di rilascio delle autorizzazioni nazionali al trasferimento dei dati personali tramite *Bcr*, soprattutto con riferimento alla fase di *"cooperazione"* tra le Autorità in materia di protezione dei dati prevista dai documenti del Gruppo art. 29 (*cfr.* WP 107 e WP 133). L'applicazione concreta ha, infatti, reso evidente l'opportunità di prevedere meccanismi di cooperazione più rapidi e trasparenti, in grado di velocizzare anche i tempi di definizione delle procedure di autorizzazione. È stata, in questo senso, intrapresa un'attività di revisione del WP 107, volta a migliorarne l'efficacia.

In tale linea alcune Autorità, tra cui il Garante, hanno aderito ad un accordo volto alla predisposizione di una procedura di *"stretta cooperazione"* in materia di procedura di rila-

scio delle autorizzazioni ai trasferimenti di dati personali tramite *Bcr*, con l'obiettivo di semplificare gli adempimenti posti a carico delle società e di definire in tempi più rapidi le attività di analisi dei testi di *Bcr* sottoposti a valutazione.

Privacy e minori

Il Gruppo ha approvato il documento di lavoro n. 1/2008 sulla tutela dei dati relativi ai minori (WP 147).

Il documento è stato sottoposto a consultazione pubblica, e ha costituito la base del successivo parere 2/2009 (WP 160) adottato l'11 febbraio 2009.

Come nel documento di lavoro, il parere è suddiviso in due parti: la prima volta ad individuare i princìpi fondamentali in materia di protezione del minore con specifico riferimento alla tutela dei dati, e la seconda relativa all'attuazione dei princìpi di protezione dati nell'ambito scolastico, luogo assai significativo per lo sviluppo del minore e in cui si svolgono molte delle sue attività quotidiane.

Particolare attenzione è prestata al principio dell'interesse primario del minore (*cd.* "*best interest of the child*"), elemento fondamentale per la risoluzione dei conflitti che possono insorgere anche tra i minori e i loro rappresentanti. Ampio spazio è inoltre dedicato al principio di rappresentanza (da parte dei genitori o di chi abbia titolo) nonché alla necessità che nelle decisioni concernenti il minorenne si tenga conto del suo livello di maturità, coinvolgendolo progressivamente nelle scelte che lo riguardano.

Con specifico riferimento alla protezione dei dati, il parere ricorda che i princìpi di protezione dati e, in particolare, di qualità dei dati, di correttezza e di proporzionalità del trattamento devono essere rispettati soprattutto laddove il trattamento riguardi i minori. A tal proposito viene anche menzionato il diritto all'oblìo, particolarmente significativo considerato che le informazioni che riguardano il minorenne sono suscettibili di divenire presto obsolete ed eccedenti rispetto all'originario scopo della raccolta.

Con riferimento all'informativa, il parere si sofferma sulla necessità di utilizzare criteri di sinteticità e di semplicità in grado di accrescere, con un linguaggio adeguato, la consapevolezza del minore sul trattamento dei dati che lo riguardano.

La seconda parte del parere riguarda principalmente l'applicazione delle regole in materia di protezione dei dati nelle scuole. In particolare, sono enunciati i princìpi ai quali si

devono ispirare i trattamenti dei dati che confluiscono nei *dossier* scolastici suscettibili di causare discriminazione tra gli studenti. Il parere si sofferma inoltre sulla comunicazione a soggetti terzi da parte delle scuole dei dati relativi agli alunni per finalità di *marketing*, nonché sulla disciplina dei risultati scolastici, caratterizzata da una certa difformità tra gli Stati membri che optano per il principio di trasparenza dei risultati e quelli che ne privilegiano invece la confidenzialità.

Grande attenzione è prestata all'impiego delle nuove tecnologie nella vita scolastica. L'impiego di dispositivi biometrici per l'accesso alle scuole, di videosorveglianza, e di *badge* muniti di *Rfid* devono ispirarsi al rigoroso rispetto del princìpi di necessità e di proporzionalità, anche tenendo conto che forme di controllo eccessive possono incidere sullo sviluppo del minore stesso.

Vengono dettati princìpi sull'uso di siti *web* scolastici, sulla pubblicazione di foto di minori anche su Internet, e apposite precauzioni per l'uso di videofonini.

Il parere richiama l'attenzione dei diversi soggetti coinvolti (insegnanti, scuole, autorità competenti, *ecc.*) sulla necessità di garantire un'adeguata protezione dei dati relativi ai minori e di avviare un processo di sensibilizzazione dei minori stessi riguardo ai rischi derivanti dal trattamento dei dati che li riguardano e all'esercizio dei loro diritti.

Protezione dei dati e attività dei motori di ricerca

Del parere del 4 aprile 2008 (WP 148), sulla protezione dei dati in relazione alle attività dei motori di ricerca si è riferito nella *Relazione* 2007 (*p.* 164).

Dopo la pubblicazione del parere tutti i principali gestori dei motori di ricerca hanno contattato il Gruppo per manifestare la propria disponibilità a valutare con attenzione le indicazioni fornite dalle autorità europee. *Google*, inoltre, ha iniziato un dialogo molto serrato con il *Data Protection Commissioner* irlandese, avendo stabilito in Irlanda il proprio *data center*. Attraverso tale dialogo, *Google* ha inteso affrontare in modo dettagliato molte delle questioni sulle quali il Gruppo aveva sollecitato una presa di posizione da parte dei motori di ricerca. Le risposte di *Google* si sono concretizzate in una *"lettera aperta"* in cui l'azienda informava di aver ridotto il periodo di conservazione dei *file* di *log* degli utenti da diciotto a nove mesi, per venire incontro alle sollecitazioni del Gruppo art. 29 (che comunque aveva indicato un periodo non superiore ai sei mesi). *Google*

affrontava tutti i punti sollevati nel parere del Gruppo art. 29 sui *"motori di ricerca"*, con particolare riguardo alla natura di dato personale dell'indirizzo Ip (contestata da *Google*, che comunque non escludeva la necessità di un'analisi specifica, caso per caso, al fine di valutare l'effettiva rintracciabilità dell'interessato attraverso l'indirizzo Ip); all'applicazione delle disposizioni della Direttiva 2002/58/Ce rispetto ai *cookie* utilizzati per tenere traccia degli utenti ed alla titolarità del trattamento (*Google Inc.* non riteneva che i trattamenti effettuati dalle controllate europee, principalmente per finalità di natura commerciale, consentissero di estendere le norme della direttiva Ue ai trattamenti effettuati attraverso il motore di ricerca, pur riconoscendo che vi è un margine di apprezzamento in materia); alla liceità delle operazioni di trattamento effettuate da *Google*. Il Gruppo art. 29 ha quindi deciso di tenere un'audizione pubblica per sollecitare chiarimenti su queste ed altre problematiche (*ad es.*, le modalità di anonimizzazione delle stringhe di ricerca), invitando i principali gestori di motori di ricerca (*Google*, *Yahoo!* e *Microsoft*) ed un meta-motore di ricerca (*Ixquick*); l'audizione si è tenuta durante la riunione plenaria del febbraio 2009.

Il Gruppo si è successivamente dato alcune settimane di tempo per riflettere sulle risposte fornite e valutare l'opportunità di altre iniziative congiunte. Va rilevato che nel frattempo anche *Microsoft* e *Yahoo!* hanno segnalato la propria disponibilità a ridurre i tempi di conservazione dei *file* di *log* degli utenti, pari a diciotto mesi per quanto riguarda *Microsoft* (che si è dichiarata disposta a scendere a sei mesi) e a novanta giorni per quanto concerne *Yahoo!* (anche se i *log*, di fatto, vengono conservati in forma non anonima per sei mesi per finalità di lotta contro frodi ed altre forme di criminalità).

Privacy e comunicazioni elettroniche

Come accennato nella *Relazione* 2007 (*v. p.* 165), il Gruppo art. 29 si è occupato delle proposte di revisione della Direttiva 2002/58/Ce, presentate dalla Commissione il 13 novembre 2007, in materia di *privacy* e comunicazione elettroniche. Va sottolineato che il pacchetto di proposte della Commissione comprendeva anche una *"proposta di Regolamento"* concernente l'istituzione di un'Autorità europea di regolazione del mercato delle comunicazioni, fra i cui compiti rientrerebbe la definizione di *standard* di sicurezza paneuropei (con ciò accogliendo in parte la proposta formulata dal Gruppo art. 29 nel suo