L'articolo 13 della l. n. 689/81 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 Srato 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 invece 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 finale 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 2015 hanno riguardato:

- l'omessa o inidonea informativa – art. 161 (n. 223);
- il trattamento illecito amministrativo – art. 162, comma 2-*bis* (n. 1.350);
- l'utilizzo illecito dei dati delle persone iscritte al Registro pubblico delle opposizioni per finalità di *marketing* – art. 162, comma 2-*quater* (n. 5);
- l'omessa o incompleta notificazione – art. 163 (n. 44);
- l'omessa adozione delle misure minime di sicurezza di cui all'art. 33 del Codice – art. 162, comma 2-*bis* (n. 21);
- la conservazione di dati di traffico telefonico e telematico per un tempo superiore a quello srabilito dall'art. 132 del Codice – art. 162-*bis* (n. 9);
- l'omessa informazione o esibizione al Garante – art. 164 (n. 28);
- l'inosservanza di un provvedimento del Garante – art. 162, comma 2-*ter* (n. 10);
- la violazione di disposizioni del Codice in relazione a banche dati di particolari rilevanza o dimensioni – art. 164-*bis*, comma 2 (n. 6).

Un approfondimento merita il dato relativo alle 1.350 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 disposizioni del Codice, estremamente eterogenee, e, in particolare, gli artt: 17 (verifica preliminare), 18, 19, 20, 21, 22, commi 8 e 11 (disposizioni 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 specifi-

che per le comunicazioni elettroniche). Nel 2015 le violazioni concernenti il "trattamento illecito amministrativo" accertate hanno riguardato:

- in 1.270 casi, la violazione del consenso dell'interessato in rapporto agli artt. 23 e 130 del Codice. In particolare, occorre evidenziare che è stata effettuata, grazie alla collaborazione con la Guardia di finanza, un'attività straordinaria nei confronti dei soggetti operanti nel settore del *money transfer*, che ha condotto alla contestazione di n. 1.172 violazioni nei confronti delle società coinvolte. Dagli accertamenti è emerso che tali società utilizzavano illecitamente i dati di centinaia di persone o clienti ignari per frazionare fittiziamente il trasferimento all'estero di ingenti somme di denaro ed eludere così i limiti che impongono agli operatori la segnalazione, agli enti preposti per i controlli antiriciclaggio, di transazioni monetarie al di sopra di certe soglie (cfr. *newsletter* del Garante n. 406, 28 settembre 2015 doc. web n. 4277760);
- in 38 casi, violazioni commesse da enti pubblici (nella maggior parte dei casi comunicazioni o diffusioni di dati personali comuni senza i necessari presupposti di legge o regolamento);
- in 5 casi, violazioni delle misure e degli accorgimenti prescritti dal Garante nell'ambito di una verifica preliminare sulla base dell'art. 17 del Codice;
- in 18 casi, violazioni commesse da enti pubblici con riferimento a dati sensibili o giudiziari;
- in 3 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 5 casi, violazioni commesse da soggetti privati o pubblici in relazione alle ulteriori garanzie previste dall'art. 26 del Codice per il trattamento di dati sensibili;
- in 15 casi, violazioni commesse da fornitori di reti pubbliche di comunicazione o di servizi di comunicazione elettronica con riferimento all'effettuazione di comunicazioni indesiderate.

Analizzando i dati statistici sopra riportati si può rilevare che:

- in senso assoluto, per l'anno di riferimento, il numero di violazioni accertate in merito all'obbligo di fornire all'interessato tutte le informazioni sul trattamento dei dati, non è srata la violazione più ricorrente, a differenza che negli anni precedenti;
- la violazione maggiormente riscontrata è risultata quella relativa alla mancata acquisizione del consenso degli interessati; sono state riscontrate in merito quasi 1.300 violazioni, in parte legate all'effettuazione di comunicazione indesiderate, mentre, per larghissima maggioranza, le stesse sono state riscontrate, come accennato, nell'ambito di una vasta operazione condotta dalla magistrarura nei confronti di alcune società di *money transfer* che utilizzavano i dati personali di clienti inconsapevoli.

I procedimenti sanzionatori definiri nell'anno 2015 con provvedimento di ordinanza adottato dall'Autorità, relativamente a violazioni contestate negli anni precedenti al 2015 e non definite all'epoca attraverso il pagamento spontaneo in misura ridotta da parte del contravventore, sono stati 386. Di questi, 294 hanno comportato l'applicazione di una sanzione (per un ammontare complessivo di somme ingiunte pari a 3.013.000 euro) e 92 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 adottate, quelle più significative, sotto il profilo della rilevanza degli aspetti giuridici, sono brevemente riassunte di seguito.

- Applicabilità delle tutele del Codice nei casi di comunicazioni indesiderate effettuate nei confronti di persone giuridiche. Nel caso in cui i trattamenti di dati personali effettuati dal titolare siano riconducibili all'ambito di applicazione di quelli previsti dall'art. 130, comma 1, del Codice, ai fini dell'attribuzione della responsabilità dell'illecito amministrativo derivante dalla disapplicazione dell'istituto del consenso, non si può fare riferimento alla definizione di interessato di cui all'art. 4, comma 1, lett. *i*) del Codice (i.e, "persona fisica cui si riferiscono i dati personali") bensì a quella di "contraente" prevista dall'art. 4, comma 2, lett. *f*), del Codice, che include anche le persone giuridiche. Ne discende che, nelle ipotesi di cui al cit. art. 130, comma 1, la tutela del dato personale ricomprende anche la persona giuridica-contraente e che la mancata acquisizione del consenso della stessa al trattamento configura una violazione del Codice (ordinanza-ingiunzione 7 maggio 2015, n. 276, doc. web n. 4207931).
- Deroga del Codice al principio di personalità di cui agli artt. 2 e 3, l. n. 689/1981. Riguardo il principio di personalità di cui agli artt. 2, 3 e 7, l. n. 689/1981, si evidenzia come la disciplina dettata dal Codice costituisca *lex specialis* rispetto alle previsioni della predetta legge, in quanto quest'ultima risulta essere una fonte di pari grado, richiamabile, per effetto dell'art. 166 del Codice, solo "in quanto applicabile". Il Codice dispone che gli adempimenti siano posti in essere, in primo luogo, dal titolare del trattamento, che, secondo quanto previsto all'art. 28 del Codice – quando il trattamento è effettuato da una persona giuridica, da una p.a. o da un qualsiasi altro ente, associazione od organismo – risulta essere "l'entità nel suo complesso", ferma restando la facoltà in capo allo stesso, nell'ambito del potere di organizzazione del trattamento dei dati, di delegare l'assolvimento di taluni adempimenti anche a persone (fisiche o giuridiche) individuate, ai sensi dell'art. 29 del Codice, quali responsabili del trattamento (ordinanza-ingiunzione 29 gennaio 2015, n. 51, doc. web n. 3925407).
- Ambito di applicazione dell'art. 13, comma 5-*bis* del Codice. Quando l'invio dei *curricula* avviene a fronte della pubblicazione di inserzioni su quotidiani e periodici di annunci ed offerte di lavoro, tale invio non può essere considerato spontaneo ai sensi dell'art. 13, comma 5-*bis* del Codice, bensì sollecitato dal titolare del trattamento, come, peraltro, esplicitato nel parere del Garante del 10 gennaio 2002, e quindi sottoposto agli obblighi previsti dal Codice, con particolare riferimento all'informativa agli interessati (ordinanza-ingiunzione 5 marzo 2015, n. 132, doc. web n. 3999100).
- Ambito di definizione del titolare del trattamento. L'operazione di pubblicazione in elenco telefonico di numerazioni mobili, benché effettuata dal *dealer* in fase di attivazione delle sim, deve essere imputata all'operatore telefonico, in qualità di titolare del trattamento. Ciò vale aldilà della formale qualifica di titolare del trattamento, attribuita al *dealer* nel contratto stipulato con l'operatore telefonico. Infatti, i poteri previsti dal Codice per l'esercizio della titolarità comprende, in primo luogo, quello relativo "[al]le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati" (artt. 4, comma 1, lett. *f*) e 28 del Codice). Nel caso specifico, avendo l'operatore telefonico adottato autonomamente ogni determinazione in ordine alla predisposizione dei moduli e della contrattualistica da presentare ai clienti per le attivazioni telefoniche, il *dealer* è obbligato a seguire dettagliatamente le istruzioni impartite e ad attenersi alle indicazioni operative di volta in volta decise proprio dall'operatore

telefonico (ordinanza-ingiunzione 18 giugno 2015, n. 362, doc. web n. 4253116).

- Rapporto tra titolare e responsabile del trattamento. A fronte di un'attività di polizia giudiziaria, nell'ambito della quale sono state individuate delle responsabilità penali in capo a un funzionario e al direttore di una filiale bancaria per aver attivato due conti correnti all'insaputa dell'interessato, il Garante ha stabilito che, sotto il profilo della protezione dei dati personali, le responsabilità connesse agli adempimenti in materia di informativa e consenso devono, nel caso di specie, essere imputate alla banca che, in qualità di titolare del trattamento, adotta ogni decisione in merito alle finalità e alle modalità del ttattamento, agli strumenti utilizzati, anche "sotto il profilo della sicurezza". Pertanto, anche in presenza delle designazioni dei direttoti di filiali e dei funzionari quali responsabili e/o incaticati del trattamento, ai sensi degli artt. 29 e 30 del Codice, la responsabilità per i fatti oggetto di contestazione va individuata in capo alla banca che ha omesso di vigilare sull'osservanza delle proprie istruzioni (ordinanza-ingiunzione 11 giugno 2015, n. 348 doc. web n. 4243123).

L'ammontare dei pagamenti effettivamente effettuati nell'anno 2015 da parte dei soggetti nei cui confronti sono srati avviati procedimenti sanzionatoti amministrativi è risultato complessivamente pati a 3.345.515 euro (cfr. sez. IV, tab. 8) di cui:

- 1.647.468 euro, pagati a titolo di definizione in via breve;
- 1.170.930 euto, 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;
- 270.000 euro, per la definizione, in sede amministtativa, dei procedimenti relativi alla mancata adozione delle misure minime di sicurezza;
- 257.117 euro, quali ulterioti entrate derivanti dall'attività sanzionatotia (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 artività ispetriva e di divulgazione della disciplina della protezione dei dati personali.

22 Le relazioni comunitarie e internazionali

Nel 2015, è proseguita l'intensa attività del Garante a livello europeo ed internazionale (cfr. sez IV, tab. n. 20).

Nell'ambito della modernizzazione degli strumenti normativi in materia di protezione dei dati personali si è giunti alla conclusione dell'*iter* legislativo europeo per la definizione del cd. pacchetto protezione dati, che si compone di una proposta di regolamento, volta a disciplinare i trattamenti di dati personali sia nel settore privato sia nel settore pubblico e destinata a sostituire la direttiva 95/46/CE, e di una proposta di direttiva indirizzata alla regolamentazione dei settori di prevenzione, contrasto e repressione dei crimini, nonché all'esecuzione delle sanzioni penali, che sostituirà ed integrerà la decisione quadro 977/2008/GAI (che l'Italia non ha ancora attuato).

La riforma presenta diverse novità e comporta un ripensamento dell'intera architettura normativa ed organizzativa della protezione dati (per un quadro sinterico dei due strumenti, con particolare attenzione alle novità introdotte rispetto all'attuale quadro normativo, v. par. 22.1).

Il 2015 è stato anche contrassegnato dagli importanti contributi della CGUE volti a chiarire il quadro applicativo della disciplina in materia di protezione dei dati. Di particolare rilevanza è stata la sentenza del 6 ottobre 2015 (causa C-362/14; cd. caso Schrems), nella quale la Corte ha dichiarato l'invalidità della decisione 2000/520/CE della Commissione del 26 luglio 2000 che aveva attestato che gli Stati Uniti, attraverso il cd. *Safe Harbor* (sistema per il trasferimento dei dati verso gli USA, applicabile alle sole imprese che lo sottoscrivono), garantiscono un adeguato livello di protezione dei dati personali trasferiti.

La vicenda all'origine del giudizio della CGUE inizia nel giugno del 2013, quando uno studente di giurisprudenza austriaco chiede all'autorità di protezione dei dati irlandese di ordinare a Facebook di sospendere il trasferimento dei dati personali dei propri utenti europei negli Stati Uniti, che – a seguito delle rivelazioni di Snowden – non potevano considerarsi in grado di garantire adeguatamente il rispetto del diritto alla protezione dei dati e della vita privata. La Corte di giustizia, investita della questione pregiudiziale dall'Alta Corte di giustizia irlandese, ha in primo luogo reputato che l'esistenza di una decisione della Commissione che dichiara che un Paese terzo garantisce un livello di protezione adeguato non può sopprimere né ridurre i poteri delle autorità nazionali di controllo: queste ultime devono anzi poter esaminare, in piena indipendenza, se il trasferimento rispetti i requisiti della direttiva e, in caso ritengano che la decisione della Commissione sia invalida, rivolgersi ai giudizi nazionali affinché questi ultimi possano rinviare la causa dinanzi alla Corte di giustizia.

La sentenza ha inoltre ritenuto che nella suddetta decisione la Commissione ha omesso di effettuare una valutazione circa l'adeguatezza del sistema legislativo statunitense e degli impegni internazionalmente assunti (essa infatti non menziona l'esistenza, negli Stati Uniti, di norme intese a limitare le ingerenze da parte di autorità pubbliche che vadano oltre quanto previsto in una società democratica, né l'esistenza di una tutela giuridica efficace contro tali ingerenze), limitandosi invece ad esaminare il regime del *Safe Harbor*, applicabile alle sole imprese che lo sottoscrivono e non alle autorità pubbliche. Secondo la Corte una normativa che consenta alle autorità pubbliche di accedere in maniera generalizzata al contenuto di comu-

nicazioni elettroniche deve essere considerata lesiva del diritto fondamentale al rispetto della vita privara. Nella valurazione d'adeguatezza è inoltre di cruciale importanza il riconoscimento di una tutela giurisdizionale effettiva.

La decisione della Corte è stara al centro di un'intensa attività del Gruppo Art. 29 volta ad approfondite i riflessi della sentenza sul piano nazionale ed europeo anche al fine di costituire una posizione comune delle autorirà per una sua corretta applicazione (v. par. 22.3).

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

L'*iter* legislativo europeo che ha portato alla definizione del cd. pacchetto protezione dati composto dal regolamento generale sulla protezione dei dati e dalla direttiva sulla protezione dati nelle attività giudiziarie e di polizia è stato particolarmente lungo e faticoso.

Parlamento europeo e Consiglio UE, che partecipano su un piano paritario alla procedura di co-legislazione (definita "ordinaria" in base al TFUE), hanno presentato in questi anni numerosi emendamenti ai testi proposti dalla Commissione. Diversi sono stati anche i contributi sottoposti all'attenzione dei legislatori dal Gruppo Art. 29, che ha licenziato numerosi pareri e documenti sia sull'intera riforma sia su singole tematiche (v. *infra*), e dal Garante europeo per la protezione dei dari.

Il Parlamento europeo aveva concluso la prima lettura il 12 marzo 2014, votando su entrambi i testi, mentre l'esame da parte del Consiglio UE (gruppo di lavoro DAPIX) è srato molto più lungo e complesso, tanto che l'adozione in prima lettura da parte del Consiglio "Giustizia e affari interni" si è avuta solo nel giugno 2015 per la proposta di regolamento e nell'ottobre 2015 per la proposta di direttiva. Sono stati successivamente ed immediatamente avviati i cd. "triloghi" interistituzionali (Parlamento-Consiglio-Commissione) nei quali la Presidenza di turno del Consiglio UE ed i relatori del Parlamento europeo, assistiti dalla Commissione, hanno esaminato i punti di divergenza e individuato possibili testi di compromesso per i due strumenti. Tali testi sono stati infine approvati per il Consiglio dal COREPER il 16 dicembre, e il 17 dicembre per il Parlamento dalla competente Commissione LIBE (Libertà dei cittadini e diritti fondamentali) che ha accettato il testo votaro dal COREPER il giorno precedente, cosicché il Consiglio ha ratificato l'accordo politico con il voto definitivo del COREPER del 18 dicembre. L'*iter* legislativo si è concluso il 14 aprile 2016 con l'approvazione senza modifiche da parte del Parlamento UE di entrambi i testi in seconda lettura e con la formale presa d'atto del Consiglio UE in data 21 aprile 2016 (la pubblicazione è prevista sulla GUUE del 4 maggio 2016).

Sul piano dei contenuti, numerose sono le novità introdotte dai due strumenti rispetto all'esistente quadro normativo. Questo ha infatti indotto a prevedere un periodo di due anni ai fini dell'applicazione del regolamento dopo la sua entrata in vigore (con la pubblicazione sulla GUUE); identico periodo è previsto per la trasposizione della direttiva da parte dei legislatori nazionali, fissato in 2 anni dalla dara di pubblicazione, in modo che entrambi gli strumenti siano applicati contemporaneamente dagli Stati dell'Unione. Si può dunque affermare che l'orizzonte temporale di completamento della cd. fase discendente della riforma si collochi nella primavera-estate del 2018.

Regolamento UE protezione dati

Riguardo al regolamento, il testo si articola su 11 Capi, con 99 articoli e 173 "considerando". L'impianto concettuale e giuridico dell'attuale direttiva 95/46/CE (che sarà abrogata alla data di applicazione del regolamento) trova sostanziale conferma. I princìpi fondamentali del trattamento (qualità dei dati, presupposti di liceità), i diritti degli interessati (in particolare, informativa e accesso, consenso, ret-

tifica e opposizione), l'esistenza di autorità incaricate specificamente di garantire il rispetto della normativa restano pilastri essenziali anche nella riforma, trovando peraltro fondamento negli artt. 7 ed 8 della Carta dei diritti fondamentali dell'UE. Il regolamento dà tuttavia ulteriore enfasi ad alcuni di tali elementi e introduce, per altro verso, componenti innovative, di cui si danno nel prosieguo le linee essenziali.

Diritti degli interessati:

- potenziamento dei contenuti obbligatori dell'informativa (con possibilità per i titolari di ricorrere ad icone o forme grafiche di informativa in associazione all'informativa testuale vera e propria);
- introduzione del diritto ad una cancellazione estesa dei propri dati personali (oblio), comprendente anche copie o *link* riferiti a tali dati, ma non incondizionata, essendo previste limitazioni all'esercizio del diritto per contemperare altre esigenze e interessi legittimi (libertà di espressione, interesse pubblico, finalità archivistiche nel pubblico interesse);
- introduzione della possibilità di chiedere la "limitazione" del trattamento (anziché la cancellazione), ad esempio in attesa di definire l'esattezza o obsolescenza di un dato o per continuare ad utilizzare il dato per specifiche finalità, in particolare giudiziarie;
- introduzione del diritto alla portabilità dei dati (riferito ai dati forniti direttamente dall'interessato, sulla base del consenso o di disposizioni contrattuali), con alcune eccezioni, in particolare per i dati contenuti in archivi di interesse pubblico;
- previsione di una forma di consenso rafforzato (non solo "inequivocabile", ma anche "esplicito") qualora vi si ricorra per legittimare il trattamento di dati sensibili;
- definizione di condizioni restrittive (intervento obbligatorio dei soggetti che detengono la potestà genitoriale) ai fini della valida prestazione del consenso da parte di minori in rapporto all'offerta di "servizi della società dell'informazione"; la soglia di età relativa alla minorità è fissata fra i 13 ed i 16 anni, e la scelta in merito è rimessa al legislatore nazionale.

Obblighi dei titolari di trattamento:

- introduzione del cd. "approccio basato sul rischio" e, più in generale, del principio di *accountability* ovvero di responsabilizzazione dei titolari di trattamento. Ciò si traduce in una ampia serie di disposizioni che tendono a promuovere approcci proattivi, e non reattivi, in un'ottica di prevenzione di possibili problematiche e di riduzione degli oneri considerati puramente burocratici, quali la notifica dei trattamenti. Ricordiamo le principali:

a) applicazione dei princìpi di *privacy by design* e *privacy by default* in via generale;
b) obbligo per tutti i titolari/responsabili di condurre una valutazione di impatto prima di procedere ad un (nuovo) trattamento, seguita eventualmente dalla consultazione dell'Autorità di controllo qualora il titolare non ritenga sufficienti le misure di mitigazione del rischio a lui note o disponibili;
c) introduzione e disciplina della figura del "Responsabile della protezione dati" (ovvero il *Data Protection Officer*), la cui nomina è obbligatoria per i soggetti pubblici, mentre è facoltativa per i soggetti privati ad eccezione di alcuni trattamenti particolarmente a rischio e salva diversa disposizione della legislazione nazionale. Il regolamento fissa i requisiti essenziali in termini di indipendenza, conoscenze e compiti del DPO;
d) disciplina specifica della contitolarità di trattamento e della ripartizione di

responsabilità fra contitolari, e specificazione del vincolo di natura contrattuale che deve sussistere fra titolare e responsabile del trattamento;

e) eliminazione dell'obbligo di notifica dei trattamenti all'Autorità (sostituita dall'obbligo di tenuta di documentazione sui trattamenti svolti, a disposizione dell'Autorità);

f) introduzione dell'obbligo generalizzato per tutti i titolari di notificare eventuali violazioni di dati personali (*personal data breach*), all'Autorità ed agli interessati, secondo un criterio di rischio più o meno elevato per i diritti dell'interessato stesso;

g) potenziamento del ricorso a codici deontologici (anche settoriali) e introduzione dell'istituto della certificazione dei trattamenti, entrambi utilizzabili anche ai fini di trasferimenti di dati in Paesi terzi; in questo contesto, il regolamento assegna alle Autorirà di conrrollo un ruolo non esclusivo di monitoraggio dell'attuazione e del rispetto di codici deontologici e schemi di certificazione, lasciando spazio anche a soggetti privati a ciò abilitati o accreditati.

Governance della protezione dari:

- definizioni dettagliate di ruolo e poteri delle Autorità nazionali di controllo (discendenti direttamente dal regolamento e non dal diritto nazionale);
- previsione di veri e propri obblighi di cooperazione fra Autorità nazionali con possibilità di svolgere ispezioni e indagini congiunte sul rispettivo territorio nazionale;
- in contesti di trattamento di natura multinazionale, introduzione del meccanismo dello "spottello unico" per i titolari/responsabili di trattamento (salva la competenza esclusiva dell'Autorità nazionale per trattamenti svolti da soggetti pubblici nazionali) e del "meccanismo di coerenza".

a) Ciò si concretizza nella previsione della figura della "Autorità capofila", sostanzialmente l'Autorità competente sullo stabilimento principale (o unico) del titolare/responsabile nell'UE; a tale Autorità è rimessa la decisione ultima (ad es., per quanto riguarda l'adozione di codici deontologici, clausole contrattuali, *Binding corporate rules*, o la composizione di contenziosi) anche se attraverso un processo di codecisione cui partecipano tutte le altre Autorità "interessate" a vario titolo nell'UE. Vi è poi una riserva di competenza dell'Autorità nazionale (non capofila) rispetro a "reclami" che si dimostrino avere carattere esclusivamente nazionale, e quindi risultino privi di ripercussioni su altri Stati membri; in caso di controversie fra, in particolare, l'Autorità capofila e le altre Autorità interessate, interviene il Comitato europeo della protezione dei dati con funzione dirimenre;

b) definizione di funzioni, poteri e ruolo del "Comitato europeo della protezione dei dati" quale garante di coerenza e armonizzazione. Tale Comitato è l'erede dell'attuale Gruppo Art. 29, formato da rappresentanti delle Autorità di controllo nell'UE, ma le sue caratteristiche ne travalicano considerevolmente gli ambiti. Si tratta infatti di un soggetto dotato di personalità giuridica, con una presidenza ed un segretariato permanente, incaricato di redigere e diffondere Linee guida, direttive, pareri su molteplici aspetri sostanziali e procedurali del regolamento, e avente il ruolo di decisore ultimo vincolante in caso di controversie fra Autorità nella trattazione di casi gestiti secondo il meccanismo di coerenza e/o attraverso il meccanismo dello "sportello unico" (codecisione uniforme);

c) definizione di un sistema unificato europeo di sanzioni amministrarive

(pecuniarie) che le Autorità di controllo hanno il potere di comminare in aggiunta a o in sostituzione dei provvedimenti assunti in base ai poteri loro conferiti dal regolamento. Tali sanzioni sono distribuite secondo tre diversi livelli di gravità delle violazioni (con importi pecuniari rispettivamente fissati in termini di massimo edittale); nel testo del regolamento sono indicati specifici criteri (attenuanti/aggravanti) per la definizione della gravità della violazione da parte delle Autorità di controllo, suscettibili di integrazioni ad opera del Comitato europeo della protezione dei dati.

In termini generali, altri elementi importanti da segnalare:

- campo di applicazione territoriale e materiale del regolamento: ai fini dell'applicazione delle disposizioni contenute nel regolamento, viene meno il criterio di collegamento basato sull'utilizzo di "strumenti" situati nel territorio UE da parte di titolari non stabiliti in un Paese UE (Art. 4(1)c della direttiva 95/46; art. 5, comma (2) del Codice italiano), poiché si introduce il criterio del *targeting* (offerta di prodotti o servizi destinati a soggetti presenti nell'UE). Tale disposizione mira a garantire che le tutele offerte dalla legislazione UE trovino applicazione ai dati oggetto di trattamento *tout court*, senza riguardo, quindi, a fattori di natura materiale. La tutela in questione non riguarda solo i "cittadini" dell'UE, ma, appunto, chiunque si trovi nell'UE e sia destinatario di tali prodotti o servizi (in conformità degli artt. 7 e 8 della Carta dei diritti fondamentali).
- Previsione di un margine di flessibilità lasciato agli Stati membri per alcune tipologie di trattamento, in particolare i trattamenti svolti per finalità di "pubblico interesse" o "in adempimento di un obbligo legale" nonché per i trattamenti di cui al Capo IX (giornalismo, lavoro, ricerca scientifica, statistica, storica, archivi). Si tratta di un elemento piuttosto peculiare in uno strumento, quale il regolamento, la cui *ratio* consiste proprio nel superare divergenze e differenze legate al diritto nazionale; purtuttavia, l'introduzione di questi ampi margini di flessibilità trova giustificazione nell'esistenza di un quadro molto articolato di norme nazionali che, soprattutto in alcuni settori e in alcuni Paesi (fra cui il nostro), già contengono numerose salvaguardie per la tutela dei dati personali e costituiscono uno sviluppo importante oltre che il frutto dell'esperienza applicativa raccolta in questi ultimi venti anni. Negli ambiti sopra ricordati, gli Stati membri sono pertanto autorizzati a "introdurre o mantenere" disposizioni di diritto nazionale che consentano di "adattare" quelle contenute nel regolamento. Tale rinvio espresso al legislatore nazionale è accompagnato da un elenco dei requisiti sostanziali che devono essere soddisfatti da ogni misura legislativa nazionale cui si ricorra in questi settori: specificazione delle finalità perseguite; dimostrazione della necessità del trattamento; specificazione ulteriore delle condizioni generali di liceità; indicazione delle tipologie di dati oggetto di trattamento, degli interessati e dei destinatari eventuali dei dati; previsioni sui periodi di conservazione; norme sostanziali e procedurali per garantire, in particolare, liceità e correttezza dei trattamenti in questione.
- Occorre rilevare, inoltre, che il regolamento fa rinvio al legislatore nazionale con riguardo a ulteriori tipologie di trattamento: in particolare in ambito sanitario e rispetto ai trattamenti di dati genetici o biometrici (con possibilità di prevedere condizioni o limitazioni ulteriori); quanto ai criteri di nomina di un DPO, ampliabili ai sensi del diritto nazionale; rispetto alla possibilità di richiedere autorizzazioni da parte dell'Autorità di controllo per taluni trattamenti a rischio; con riguardo alle norme che devono disciplinare

istituzione e componenti delle Autorità di controllo ed alla possibile previsione di sanzioni, anche penali, ulteriori rispetto a quelle contenute nel regolamento. D'altro canto, si deve ricordare che il regolamento prevede espressamenre, come già la direttiva 95/46 al suo art. 13, la possibilità di introdurre con legge nazionale deroghe ai diritti degli interessati per specifiche finalità (interesse pubblico, sicurezza pubblica, sicurezza dello Stato, salute pubblica, ecc.), purché tali deroghe siano necessarie e proporzionate e, in particolare, rispettino l'"essenza" del diritto alla protezione dei dati. Significativamente, quest'ultima condizione riflette il linguaggio utilizzato dalla CGUE nella richiamata sentenza sulla tutela offerta in Paesi terzi ai dati trasferiti dall'UE (Causa C-362/14, Facebook c. Schrems, v. par. 22.3). Tale possibilità è prevista anche rispetto ai trattamenti per finalità scientifiche, statistiche, storiche, archivistiche nel pubblico interesse, salve le garanzie che il diritto nazionale deve prevedere, in particolare, l'esistenza di misure atte a favorire l'applicazione del principio di "minimizzazione dei dati".

- Un cenno specifico merita anche la materia dei trasfetimenti di dati personali verso Paesi terzi. In via generale, il regolamenro mantiene inalterati i presupposti fissati dalla direttiva 95/46: si prevede un divieto generale di trasferimento verso Paesi terzi od organismi internazionali, salva l'esistenza di una decisione di adeguatezza assunta dalla Commissione con riguardo a singoli Paesi ovvero a settori di trattamento o organismi internazionali; in assenza di una decisione del genere, è data la possibilità di ricorrere a garanzie conttattuali o ad altri presupposti in deroga, quali il consenso dell'inreressato o la prestazione contrattuale. Tuttavia, da un lato vengono irrigiditi i requisiti di adeguatezza attraverso l'obbligo per la Commissione di effettuare una valutazione complessiva, che tenga conto dell'intero quadro normativo nel Paese terzo e, quindi, anche delle tutele offerte in caso di trattamenti per finalità di polizia e giustizia e, più in generale, delle tutele esistenti rispetto ai diritti fondamentali di cui alla Carta. Per altro verso, vengono introdotte disposizioni specifiche che disciplinano l'uso di clausole contrattuali modello, norme vincolanti di impresa (Bcr) ed altre autorizzazioni di trasferimento *ad hoc* concesse dalle singole Autorità nazionali (necessariamente con intervento del "meccanismo di coerenza"). Vi è inoltre una disposizione, fortemente voluta dal Parlamento eutopeo, con cui si vietano i trasferimenti richiesti da autorità giudiziarie o amministrative di Paesi terzi qualora essi non trovino fondamento in accordi internazionali di mutua assistenza giudiziaria o in strumenti analoghi, di natura bilaterale o multilaterale.

Direttiva polizia e giustizia

Il testo della direttiva si articola in X Capi, 65 arricoli, 107 "considerando". L'impianto è sostanzialmente e strutturalmente allineato al regolamento di cui mantiene immutata l'articolazione in Capi e la corrispondenza dei titoli. I princìpi fondamentali del trattamento (liceità e correttezza, qualità dei dati, presupposti di liceità), i diritti degli interessati (in particolare, informativa e accesso, consenso, rettifica e opposizione), l'esistenza di autorità incaricate specificamente di garantire il rispetto della normativa restano pilastri essenziali anche nella direttiva, ancorché con differenze rispetto a quanto previsto dal regolamento dovute al particolare ambito disciplinato. Al riguardo va infatti considerato che – pur nell'affermazione del diritto fondamentale alla protezione dei dati, contenuta nell'art. 16 del TFUE, che costituisce peraltro la base giuridica individuata dalla Commissione per entrambi gli strumenti – la Dichiarazione 21 insisteva sulla necessità di norme specifiche per la cooperazione penale e di polizia. È per questo che, in assenza di un quadro armo-

nizzato dei princìpi di protezione dati nello specifico settore dovuta alla non completa integrazione sviluppata al riguardo, il riferimento normativo più vicino fosse alla decisione quadro n. 977 del 2008, che dettava regole sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale. È così che il tenore delle disposizioni è in parte ispirato a quelle della decisione quadro, che viene contestualmente abrogata con l'entrata in vigore della direttiva. La direttiva si pone quindi come *lex specialis* rispetto al regolamento per i trattamenti rientranti nel suo campo di applicazione. Sarà pertanto molto importante definire esattamente l'articolazione con le disposizioni del regolamento e gli ambiti di rispettiva applicazione (ad es., per le attività svolte nei settori dell'asilo, immigrazione, disciplina degli stranieri).

Il campo di applicazione materiale copre i trattamenti svolti dalle autorità competenti in base al diritto nazionale per finalità di prevenzione, indagine, accertamento e perseguimento di reati, inclusa la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica.

Le autorità competenti possono a loro volta essere sia autorità pubbliche sia qualsiasi altro organismo o entità incaricato dal diritto nazionale di esercitare l'autorità pubblica e i poteri pubblici nel settore su ricordato.

Riguardo agli aspetti più salienti, va innanzi tutto dato atto che la direttiva costituisce il primo strumento che detta regole armonizzate per i trattamenti di dati svolti dagli Stati membri nel settore "polizia e giustizia", creando vincoli certi per i legislatori nazionali, verificabili dalla Commissione e dalla stessa Corte di giustizia.

La direttiva lascia agli Stati membri la possibilità di prevedere garanzie più elevate: si tratta di un aspetto importante per la salvaguardia dei diritti fondamentali, considerando che la discussione avutasi in Consiglio ha portato ad una riscrittura in particolare degli articoli relativi ai diritti degli interessati che, prevedendo un maggior numero di deroghe, rischia di comprimere l'effettivo esercizio dei diritti di informazione, accesso, rettifica, cancellazione dei dati. Questo lascia un margine di manovra ampio agli Srati nel definire le categorie di trattamenti, il relativo rischio e le conseguenti regole. La direttiva prevede infatri che sia data una informazione molto generale sul trattamento, similmente a quanto previsto dal Codice all'art. 53, e che il legislatore individui i casi in cui debbano essere fornite informazioni più dettagliate, ciò al fine di salvaguardare le indagini ed altri aspetti di rilevante interesse pubblico. La direttiva prevede inoltre che laddove i dati personali siano trattati nell'ambito di una indagine giudiziaria penale, il legislatore debba disciplinare il modo in cui tali diritti possano essere azionabili.

Anche per quanto riguarda il trattamento dei dati sensibili – allineandosi con la decisione quadro – non c'è nella direttiva un divieto di trattamento con specificazione delle eccezioni, ma la previsione che il trattamento possa essere effettuato solo se strettamente necessatio ed in presenza di adeguate garanzie.

Relativamente agli obblighi di titolari e responsabili si segnala l'attenzione posta sulla necessità di introdurre misure di sicurezza adeguate ai rischi del trattamento. La stessa direttiva prescrive le misure da adottare in caso di trattamenti automatizzati e le elenca.

Regole simili a quelle introdotte dal regolamento vigono pet la cooperazione con l'Autorità di controllo e la definizione dei casi in cui è obbligatoria la consultazione preventiva di derta Autorità (per la notifica del *data breach*, per la tenuta dei registri e dei *log* delle operazioni).

La direttiva prevede inoltre l'obbligo di designare un "responsabile per la protezione dei dati" da parte delle autorità competenti e ne disciplina figura, compiti e risorse, indicando che può essere anche designato un unico responsabile per più

autorità competenti, tenuto conto della loro sttuttura organizzativa e dimensioni. Per quanto concerne il trasferimento di dati verso autorità competenti in Paesi terzi o otganizzazioni internazionali, le disposizioni sono allineate a quelle del regolamento per quanto concerne l'accettazione di un sistema generale basato sull'adeguatezza del Paese/organizzazione, anche se un margine più ampio è lasciato ai ttasferimenti in deroga, che comunque non devono mai essete ripetitivi o massivi. Anche gli accordi bilaterali già in vigore tra Stati UE e Paesi terzi restano tali finché non modificati. È stato inserito un articolo che, pur prevedendo una serie di stringenti condizioni, consente il trasferimento di dati personali dalle autorità competenti a soggetti privati in Paesi terzi, laddove necessario per le indagini.

I compiti ed i poteri delle Autorità di controllo sono riragliate sullo schema del regolamento, riconoscendo la tripartizione dei poteri in potere d'indagine, correttivo e consultivo effettivo, ma nella direttiva il riferimento alle attività da svolgere è molto più sintetico, ancora una volta lasciandosi spazio al legislatore nazionale.

La cooperazione delle Autorità di controllo si svolge attraverso il Comirato europeo istituito dal regolamento, cui partecipano le autorità designate dal legislatore nazionale per sorvegliare l'applicazione dei trattamenti di dati svolti nei settori ricadenti nella direttiva.

È stata inoltre inserita una disposizione che chiede al legislatore nazionale di disporre che le autorità competenti mettano in opera meccanismi efficaci per incoraggiare la segnalazione riservata di violazioni della direttiva.

22.2. *Le conferenze delle autorità su scala internazionale*

La Conferenza internazionale delle autorità di protezione dati

La 37ª Conferenza internazionale, che rappresenta 110 autorità di protezione dei dati del mondo ed esperti del settore, si è tenuta ad Amsterdam dal 26 al 29 ottobre 2015. Come negli anni precedenti, la Conferenza si è articolata in una sessione aperta, occasione di scambio con i diversi *stakeholder* sui temi di protezione dati e una sessione riservata alle sole Autorità.

Nella sessione chiusa della Conferenza sono stare presentate e adottate quattro Risoluzioni. La prima, sul tema degli accessi, da parte di autorità pubbliche, ai dati personali in possesso di società commerciali, evidenzia la necessità che sia le entità private cui le autorità si rivolgono, sia i governi adottino adeguate politiche per garantire trasparenza (cd. *transparency reporting*), in particolare sulle tipologie di richiesta e la loro base giuridica (doc. web n. 4810449).

La seconda risoluzione, sul tema *privacy* e azione umanitaria internazionale, sottolinea la necessità di garantire anche in questo settore il pieno rispetto dei princìpi di protezione dati (doc. web n. 4810431). La terza risoluzione, che è invece dedicata alla attività di cooperazione con il relatore speciale USA su diritto alla *privacy*, mira a sollecitare governi e altri attori coinvolti ad offrire il supporto necessario al relatore per adempiere alle sue funzioni (doc. web n. 4810415). Una quarta risoluzione riguarda infine la direzione strategica della Conferenza, per il periodo 2016-18 (doc. web n. 4810405).

È stata inoltre approvata una dichiarazione contenente due comunicati, rispettivamente sul tema dei dati genetici e sulla protezione dei dati nell'ambito della sicurezza e della *intelligence* (doc. web n. 4814854).

Nella sessione aperta è srato presentato il progetto *Privacy bridges*, su iniziativa dell'autorità olandese e predisposto dall'Università di Amsterdam e dal Massachusetts *Institute of Technology* di Cambridge (MA, USA), nel quale sono delineate diverse proposte per la risoluzione dei contrasti nella tutela della *privacy* e dei

dati personali tra il sistema europeo e quello statunitense. Le questioni e le 10 proposte contenute nel *Report Privacy Bridges* (doc. web n. 4814871) sono state l'oggetto principale della discussione nella sessione aperta della Conferenza.

Sempre nella sessione aperta, il Garante ha presentato la propria esperienza di cooperazione internazionale avviata con l'Albania nell'ambito dell'evento organizzato dal GPEN ("GPEN *Meeting:* 2016 *and beyond – A New Era in Global Enforcement Cooperation*") ed è stata parte attiva del *panel* "*Data Stewardship for a 21st Century Data-Driven World*", organizzato dall'*Accountability Foundation*, in particolare sul tema *big data.*

La Conferenza (attraverso il suo Comitato esecutivo) pubblica una *newsletter* per informare regolarmente in merito alle attività svolte.

La Conferenza di primavera, che riunisce le autorità di protezione dei dati personali europee si è tenuta a Manchester dal 18 al 20 maggio 2015.

La Conferenza delle autorità europee (*Spring Conference*)

Quest'anno la Conferenza dal titolo "*Navigating the Digital Future – let's get practical!*", si è concentrata sul tema dei diritti degli interessati, in particolare sugli strumenti pratici e le strategie da porre in essere per facilitarne l'esercizio, ivi compreso il rafforzamento del ruolo delle autorità di protezione dei dati nell'applicazione della normativa e delle forme di cooperazione tra le stesse autorità a livello europeo.

Nel corso della Conferenza sono state adottate tre diverse risoluzioni.

Una prima risoluzione mira a promuovere un ruolo sempre più attivo delle autorità di protezione dati per rispondere alle crescenti aspettative di tutela nel futuro digitale e richiama la necessità che le autorità di protezione dei dati siano dotate di risorse sufficienti a svolgere il loro ruolo istituzionale (doc. web n. 4810039).

La seconda risoluzione si propone invece di facilitare la cooperazione tra le stesse autorità in particolare con la predisposizione di una piattaforma web destinata a raccogliere materiali e risoluzioni della Conferenza (doc. web n. 4810056).

Con l'ultima risoluzione l'Andorra è stata accreditata tra i membri della *Spring Conference* secondo i criteri previsti dalle Linee guida per l'ammissione adottare il 23 aprile 2004 alla Conferenza di Rotterdam.

22.3. *La cooperazione tra autorità garanti nell'UE: il Gruppo Art. 29*

La prosecuzione a ritmi serrati dei lavori relativi al pacchetto europeo di riforma in materia di protezione dei dati e alcuni recenti interventi della Corte di giustizia sul tema hanno richiesto, nel 2015, una maggiore flessibilità nell'agenda delle autorità garanti nell'UE riunite nel Gruppo Art. 29. Il Gruppo (attraverso i lavori dei suoi sottogruppi e le sei riunioni plenarie tenutesi nel 2015) ha così continuato a fornire indicazioni e approfondimenti atttaverso i pareri adottati sulla base dei temi strategici fissati nel programma di lavoro relativo al biennio 2014-2015 adottato il 3 dicembre 2013 (doc. web n. 3815727). Le autorità hanno anche colto ogni possibile occasione per contribuire alla creazione di un nuovo quadro giuridico più coerente, garantista ed efficace – inviando proprie osservazioni alle tre istituzioni europee impegnate nel trilogo (v. *infra*) – e per chiarire gli effetti sull'attuale quadro normativo delle significative sentenze adottate dalla CGUE in materia di conservazione dei dati di traffico (v. sentenza Digital Rights Ireland Ltd., doc. web n. 3845166), legge applicabile (sentenze Google Spain, doc. web n. 3127044, e Weltimmo, doc. web n. 4810583) e trasferimenti di dati all'estero (sentenza Schrems, doc. web n. 4810595).

Le ripercussioni di quest'ultima sentenza (v. anche par. 22) sono state oggetto di una particolare attenzione da parte del Gruppo che – oltre ad impegnare nella sua

analisi vari sottogruppi – vi ha dedicato una sessione speciale della Plenaria tenutasi il 15 ottobre 2015. All'esito di tale plenaria, il Gruppo ha adottato una dichiarazione (doc. web n. 4810342) nella quale, oltre a dare prime indicazioni in ordine agli aspetti relativi al trasferimento di dati verso gli Stati Uniti (v. *infra*), ha anche messo in luce l'assoluta necessità di adottare una posizione comune nell'applicazione della sentenza, sottolineato come la sorveglianza massiva e indiscriminata, punto centrale della decisione della Corte, sia incompatibile con il quadro europeo, e ribadito la necessità che le istituzioni europee e gli stati membri aprano un dialogo con gli Stati Uniti per il raggiungimento di soluzioni giuridiche volte a garantire che il trasferimento dei dati oltreoceano avvenga nel rispetto dei diritti fondamentali.

Concetti chiave della direttiva – Revisione parere legge applicabile

Come anticipato, il Gruppo ha continuato ad occuparsi, nel corso dell'anno, anche di un'altra rilevante sentenza della CGUE, la sentenza del 14 maggio 2014, caso Google Spain (doc. web n. 3127044) che ha riconosciuto in capo alla società statunitense la titolarità del trattamento dei dati personali che appaiono nell'elenco dei risultati del suo motore di ricerca e l'applicabilità della disciplina europea (nel caso specifico spagnola) in materia di protezione dei dati. Con il documento del 16 dicembre 2015 (WP 179, doc. web n. 4810638) il Gruppo ha infatti aggiornato il precedente parere 8/2010 sulla individuazione della normativa applicabile in materia di protezione dei dati alla luce delle indicazioni della Corte. Il documento si è concentrato sulla parte della sentenza che ha interpretato la nozione di stabilimento prevista dall'art. 4, paragrafo 1, lettera *a*), della direttiva 95/46 e, richiamando anche la sentenza Weltimmo (doc. web n. 4810583), ha chiarito che, tra i trattamenti effettuati "nel contesto delle attività di uno stabilimento" del titolare nel territorio di uno Stato membro, rientrano anche quelli posti in essere, in un altro Stato membro, da una succursale o una filiale che svolga attività "inestricabilmente connesse" al trattamento di dati personali in questione (come tali, nel caso di Google Spain, sono considerare, ad es., il trattamento dei dati da parte di Google e la raccolta pubblicitaria effettuata dagli stabilimenti di Google in UE). Al fine di individuare la legge applicabile (o le leggi applicabili) sarà quindi necessario verificare, in ciascun caso, se le attività svolte da uno o più stabilimenti di uno stesso titolare siano "inestricabilmente connesse" al trattamento dei dati effettuato dal medesimo titolare.

Il pacchetto di riforma UE

Con riferimento al nuovo quadro posto in essere dal pacchetto di riforma sulla protezione dei dati, il Gruppo è varie volte intervenuto fornendo il proprio contributo tecnico nelle diverse fasi del processo normativo.

Rivolgendosi ai diversi interlocutori politici coinvolti nella riforma, il Gruppo (lettere 17 giugno 2015, doc. web n. 4810133) ha richiamato l'attenzione su una serie di priorità ed obiettivi da considerare nell'elaborazione dei nuovi strumenti. Secondo il Gruppo occorreva *in primis* che il pacchetto di riforma consentisse di mantenere alto il livello di protezione fino ad ora garantito dalla direttiva 95/46 e che non rappresentasse in nessun modo un ridimensionamento del sistema di tutela esistente. Riguardo ai rapporti tra i due strumenti in discussione – regolamento e direttiva sulla protezione dei dati nelle attività di contrasto – occorreva che piena coerenza fosse garantita tra i due quadri normativi, e che la proposta di direttiva rappresentasse un'eccezione ai principi del regolamento limitata esclusivamente al settore del *law enforcement* per la prevenzione e perseguimento dei reati, senza estendersi ad altre attività di autorità pubbliche. Con riferimento ai principi chiave della riforma, il Gruppo ha sottolineato che il concetto di dato personale doveva essere ampio a sufficienza da rispondere alle esigenze di protezione derivanti dalle nuove tecnologie. Occorreva inoltre una stretta osservanza del principio di finalità – che non ammette trattamenti incompatibili con gli scopi legittimi del trattamento originario – e che fossero garantiti gli strumenti necessari ad assicurare un agevole eser-

cizio dei diritti da parte degli interessati, in un quadro normativo fondato su una nuova *governance* basata sulla prossimità agli individui e sull'efficienza per il mondo delle imprese.

A tal fine, alcuni suggerimenti tecnici sono stati offerti dal Gruppo in vista del trilogo nel documento che figura in allegato alle citate lettere (doc. web n. 4810122).

Sempre con riferimento al pacchetto di riforma, il Gruppo, con una lettera del 25 settembre 2015 indirizzata alle tre istituzioni europee, ha fornito diverse osservazioni riguardo alla struttura interna del Comitato europeo della protezione dei dati (utili alla discussione nel trilogo ma anche alle future regole procedurali dello stesso Comitato) affinché tale organo abbia una struttura flessibile ed equilibrata, in grado di valorizzare la rete decentralizzata delle autorità di protezione dei dati e di fornire un efficiente e stabile coordinamento (doc. web nn. 4810318 e 4810328).

Aerei a pilotaggio remoto (RPAS)

Con riferimento alla protezione dei dati nel settore delle nuove tecnologie, il Gruppo ha portato a conclusione il lavoro di approfondimento iniziato nel 2014 su impulso della Commissione (v. Relazione 2014, p. 175) sugli aerei a pilotaggio remoto, cd. droni, per scopi civili (ivi comprese le attività di *law enforcement*). Con l'adozione del parere 1/2015 (WP231, doc. web n. 4810724) il Gruppo ha fornito indicazioni – distinguendo tra oneri e raccomandazioni per gli operatori – per consentire un utilizzo di tali mezzi rispettoso dei principi di protezione dei dati. Riguardo agli obblighi per gli operatori, il parere sottolinea la necessità di verificare la liceità del trattamento e di individuare la corretta base giuridica, di rispettare l'obbligo di fornire un'adeguata informativa tenendo conto delle peculiarità delle operazioni svolte, di osservare i principi di minimizzazione, proporzionalità e finalità del trattamento e di adottare idonee misure di sicurezza. Tra le raccomandazioni rivolte agli *stakeholder*, il parere pone invece l'accento sull'opportunità di introdurre e/o rafforzare un quadro giuridico che consenta l'utilizzo dei droni nel rispetto di tutti i diritti fondamentali, di individuare modalità di cooperazione tra autorità di protezione dei dati e autorità per l'aviazione civile in modo da richiamare l'attenzione degli operatori al rispetto delle regole in materia di protezione dei dati, di utilizzare fondi di ricerca UE per l'individuazione di strumenti tecnologicamente adeguati volti a fornire l'informativa agli interessati e favorire l'identificazione dei droni. Infine, il parere si rivolge anche a costruttori e operatori: raccomandando l'approntamento di misure di *privacy by default*, la promozione di codici deontologici, l'adozione di misure per rendere il più possibile visibile e identificabile un drone.

Le implicazioni dell'uso civile dei droni su *privacy* e protezione dei dati sono state oggetto anche di una conferenza internazionale organizzata dall'autorità ungherese (Budapest, 5-6 febbraio 2015) nella quale esperti di *privacy*, rappresentanti governativi, società civile, operatori commerciali e accademici si sono confrontati sui principi necessari a garantire un uso responsabile di tali dispositivi, nel rispetto dei diritti delle persone.

Cloud computing

Sempre nell'ambito delle nuove tecnologie con l'adozione del parere 2/2015 (WP232, doc. web n. 4810737) il Gruppo ha portato a termine il lavoro di analisi del codice di condotta europeo sul *cloud computing* predisposto dal gruppo di rappresentanti dell'industria *Cloud Select Industry Group*-CSIG. Il parere, nel ricordare che l'adesione al codice non mette le società al riparo dall'attività di *enforcement* delle autorità di protezione dei dati, si sofferma sul sistema di *governance* (che, tra l'altro, dovrà essere più stringente, attento ai cambiamenti nel quadro legislativo europeo e non prevedere la partecipazione del Gruppo Art. 29) e sulla necessità di fornire informazioni ai clienti sul luogo dove i dati verranno conservati e sulle eventuali richieste di accesso agli stessi provenienti da autorità di *law enforcement* di Paesi

terzi. Il Codice, inoltre, dovrà contenere un chiaro richiamo alla definizione di dato personale della normativa europea (ed eventualmente citare la pseudonimizzazione solo come misura di sicurezza), prevedere specifici scenari nei casi di trattamenti di dati sensibili e un regime più chiaro per l'allocazione delle responsabilità che non sia sfavorevole al cliente (titolare del trattamento). A quest'ultimo dovrà essere riconosciuto il diritto di *audit*, almeno attraverso la predisposizione da parte del fornitore del servizio *cloud di Key Performance Indicators* (KPI) e con questi il fornitore del servizio (responsabile del trattamento) dovrà cooperare per fornire all'interessato l'informativa di cui all'art. 10 e riconoscere all'interessato il diritto alla portabilità dei dati (anticipando, in questo, il regolamento).

Cookie Sweep

Il 3 febbraio 2015 è stato adottato il Rapporto dei garanti europei sull'impiego di *cookies* nell'utilizzo della rete (WP229, doc. web n. 4810673). Il Rapporto rappresenta il documento conclusivo di un'analisi congiunta (*cookie sweep*) articolata in due diverse fasi: una verifica statistica dei *cookie* utilizzati in rete e delle loro caratteristiche e una più approfondita analisi dei meccanismi di informativa e consenso in uso. Dall'esame effettuato dalle aurorità è emerso che nonostante molti operatori informino gli utenti della presenza di cookie, ancora non è frequente la raccolta di un valido consenso per il telativo trattamento dei dati, così come previsto dalla direttiva *e-Privacy* e in linea con le precisazioni finora fornite dal Gruppo Art. 29 (cfr. WP194, doc. web n. 2439391 e WP208, doc. web n. 2982826).

Dati relativi alla salute nel contesto *m-Health*

A seguito dell'adozione da parte della Commissione europea del Libro verde in materia di *Mobile Health* e per rispondere ad una specifica richiesta della stessa Commissione intesa ad ottenere un chiarimento sulla definizione di dato relativo alla salute utilizzata nel contesto delle *apps* relative a stili di vita e *well-being*, il Gruppo ha inviato una lettera alla DG-*Connect* fornendo indicazioni e chiari esempi per identificare e trattare i dati relativi alla salute anche nel contesto delle nuove tecnologie (doc. web nn. 4810096 e 4810086). Il testo distingue sostanzialmente tra tre categorie di dati raccolti attraverso tali tipologie di *app*: 1. i dati chiaramente relativi alla salute (ad es., quelli utilizzati in un contesto medico); 2. una categoria di dati che, a seconda del contesto, possono qualificarsi come dati relativi alla salute (in particolare, i dati che, seppure neutri di per sé, sono trattati per tirare conclusioni sullo stato di salute attuale o futuro); 3. esempi di dati che non costituiscono dati relativi alla salute (ad es., il dato relativo ai passi effettuati, singolarmente trattato).

Borders, Travel e Law Enforcement

Il Gruppo ha lavorato intensamente sulle implicazioni della direttiva concernente la tutela delle persone fisiche con tiguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, e la libera circolazione di tali dati (v. par. 22.1). Con il parere 3/2015 (WP233, doc. web n. 4810751) il Gruppo, partendo dal testo adottato dal Consiglio nel setrembre 2015, esprime perplessità su alcuni aspetti critici e formula suggerimenti. In particolare, il parere sottolinea la necessità di tener adeguatamente conto nel testo del fatto che il diritto alla protezione dei dati personali ha il rango di diritto fondamentale che va declinato orizzontalmente nelle varie disposizioni della direttiva in modo da garantire un livello elevato di tutela (la raccomandazione 87(15) adottata dal Comitato dei ministri del Consiglio d'Europa rappresenta al riguardo il minimo comune denominarore da garantire da parte del legislatore dell'UE). Il documento ribadisce la necessità di assicurare coerenza tra regolamento e direttiva quanto meno sui punti essenziali del disegno normativo. Quanto agli aspetti specifici, il parere considera negarivamente l'allargamento dell'ambito di applicazione materiale della direttiva volto a coprire anche la prevenzione di rischi per la sicurezza pubblica, preferendo al riguardo il testo originale della Commissione.