che, con la sentenza sulla data retention, ha sancito la centralità del diritto alla privacy nel suo rapporto con la sicurezza.

Centralità riaffermata poi, con la sentenza sull'oblio (*Costeja c. Google*) rispetto agli interessi economici dei motori di ricerca.

Sentenze coeve a quella della Corte suprema americana che, estendendo alle perquisizioni dei cellulari le garanzie previste per le limitazioni della libertà personale, ha delineato un parallelismo molto più che simbolico tra corpo fisico e corpo elettronico.

Intelligence strategica e sorveglianza di massa

Queste tre pronunce hanno in comune la qualificazione della protezione dati come principale presupposto di libertà nell'era digitale: diritto d'"inviolata personalità" senza il quale ogni democrazia rischia di cedere alla logica totalitaria dell'uomo di vetro e la rete di ridursi a dimensione anomica in cui globalizzare non le libertà, ma l'indifferenza ai diritti.

Dobbiamo contrastare la ricorrente tentazione di considerare le libertà civili come un lusso che non ci possiamo permettere di fronte alla minaccia terroristica.

È dalla centralità dell'*Habeas data* nelle nostre democrazie che deve partire l'Europa per combattere il terrorismo e ogni fondamentalismo senza rinnegare se stessa e la propria identità.

Rivedendo il rapporto tra privacy e sicurezza anche sotto il profilo della reale efficacia della sorveglianza di massa, rivelatasi assai meno utile, anche in termini investigativi, rispetto a quella "tradizionale", mirata e selettiva, come ha dimostrato la Commissione di esperti istituita da Obama.

Il modo migliore per difendere la nostra sicurezza è proteggere i nostri dati – e, con essi, le infrastrutture e i sistemi cui li affidiamo – ed evitarne raccolte massive, limitando "la superficie d'attacco" per un terrorismo che sempre più si alimenta della rete per passare dallo spionaggio informatico alla concretissima violenza delle stragi.

Un'efficace prevenzione del terrorismo dovrebbe dunque selezionare – con intelligenza, appunto – gli obiettivi "sensibili" in funzione del loro grado di rischio e fare della protezione dati una condizione strutturale di difesa dalla minaccia cibernetica, come abbiamo sottolineato anche al Comitato Schengen.

È quanto abbiamo più volte sostenuto, in primo luogo rispetto all'attività d'intelligence, soprattutto strategica che, come ha segnalato il Consiglio d'Europa, ha un raggio di azione assai più ampio e meno "puntuale" di quella tradizionale, suscettibile quindi di degenerare – se non limitato ad obiettivi realmente "sensibili" – in sorveglianza massiva.

In questo senso è particolarmente importante l'avvio di procedure informative specifiche instaurate con il Dipartimento delle informazioni per la sicurezza (Dis), al fine di assicurare la piena conformità al Codice dei trattamenti svolti dalle Agenzie di intelligence e, in tale ambito, i pareri resi quest'anno sulla disciplina delle misure di sicurezza adottate da tali organi.

Ma rischi analoghi di "sovra-acquisizione di dati" possono derivare, sia pure in misura diversa, anche dall'uso di mezzi di ricerca della prova particolarmente invasivi – ad esempio acquisizioni di tabulati o intercettazioni – se non circondati da misure di sicurezza idonee a impedire abusi o non adeguatamente circoscritti sulla base dei presupposti individualizzanti previsti dal codice di procedura penale, con il rischio di trasformarsi, così, da individuali a massivi.

Peraltro, i dati personali acquisiti con questi mezzi investigativi (ed altri: si pensi al prelievo del DNA, i cui profili confluiranno nella banca dati nazionale), vanno protetti anche successivamente alla raccolta, per impedire ogni tipo di abuso.

In tal senso vorrei sollecitare l'urgente attuazione delle misure prescritte, in particolare, al Ministero dell'interno e alle Procure della Repubblica, per garantire la sicurezza dei dati trattati nell'ambito delle rispettive funzioni.

Di questa complessiva "messa in sicurezza" dei centri, privati e pubblici, di raccolta dei dati personali, fa parte anche l'iniziativa del Garante di indicare – all'esito di attività ispettive – specifiche misure ai gestori dei principali

Nodi d'interscambio internet (IXP), per evitare che la fase di instradamento del traffico di dati verso i provider costituisca una zona "franca" e come tale vulnerabile rispetto a ogni tipo di abuso.

Che rispetto a queste strutture avrebbe effetti devastanti.

L'esperienza, anche recente, di altri Paesi europei ci rivela che questi abusi sono possibili anche in ordinamenti democratici (intercettazione dati in Germania presso il *Neutral Exchange Point* di Francoforte, 2015).

Per una trasparenza davvero democratica

Il d.lgs. 14 marzo 2013, n. 33 ha dato un importante contributo per superare la segretezza quale principale forma di esercizio del potere, mutando anche il rapporto tra singolo e autorità: da autoritativo, burocratico e insindacabile a paritetico, partecipato e "controllabile".

Tuttavia, la sua applicazione ne ha mostrato alcune criticità, legate essenzialmente al carattere indifferenziato degli obblighi di pubblicità.

Essi si applicano infatti, con analogo contenuto, ad enti e realtà profondamente diversi tra loro, senza distinzione in ragione del grado di esposizione dell'organo al rischio corruttivo; dell'ambito di esercizio della relativa azione o, comunque, delle risorse pubbliche assegnate, della cui gestione l'ente debba quindi rispondere.

Nel regolare così, in modo identico, situazioni diverse, tali norme rischiano di pregiudicare l'equilibrio complessivo della disciplina, con effetti in larga parte disfunzionali rispetto alla stessa esigenza di consentire "forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche" (art. 1, c. 1, d.lgs. 33/2013).

Pertanto, le limitazioni – spesso significative – della riservatezza, che tali obblighi di pubblicità comportano, possono risultare in alcuni casi irragionevoli e, come tali, meritevoli di revisione.

Del resto, proprio perché strumento di partecipazione, responsabilità

e legittimità, la trasparenza deve essere preservata da effetti distorsivi e da quell'"opacità per confusione" che rischia di caratterizzarla se degenera in un'indiscriminata bulimia di pubblicità.

Con il rischio di occultare informazioni realmente significative con altre inutili, così ostacolando, anziché agevolare, il controllo diffuso sull'esercizio del potere.

Quello dell'opacità per confusione è un rischio in qualche modo implicito nell'approccio scelto dal legislatore italiano, che diversamente dal Foia (*Freedom of Information Act*) ha considerato la divulgazione indiscriminata in rete quale unica modalità di assolvimento degli obblighi di pubblicità.

Va dunque ripensato non il principio di trasparenza come forma ineludibile dell'agire amministrativo, ma le modalità della sua realizzazione, anche seguendo, almeno in parte, il modello del Foia – fondato sulla legittimazione di chiunque ad accedere agli atti amministrativi su istanza di parte – e ridisegnando ambito oggettivo e contenuto degli obblighi di pubblicità, in funzione della loro reale utilità al sindacato sull'esercizio del potere.

Non sempre, infatti, la pubblicazione in rete è garanzia di reale informazione, trasparenza e quindi "democraticità", perché comporta rischi di alterazione, manipolazione, decontestualizzazione e riproduzione per fini diversi, che potrebbero frustrare ogni esigenza di informazione veritiera e, quindi, di controllo, oltre che di oblio una volta venuta meno l'utilità del dato.

Di tali esigenze ci siamo fatti portatori rispetto al Governo, anche mediante un approfondimento congiunto con l'Anac, volto a individuare possibili linee di riforma.

La sfida reale è garantire dunque una trasparenza democratica e non demagogica, utile ai cittadini e non lesiva della loro persona.

Le sentenze on-line e la trasparenza della giustizia

Analoga sinergia tra privacy e trasparenza va garantita rispetto alle sentenze on-line. La pubblicazione sul web di dati preziosi, quali quelli ricavabili da una

sentenza e dai princìpi che vi sono affermati è, infatti, indubbiamente più "democratica", perché raggiunge, potenzialmente, tutti i cittadini, mettendo a disposizione un patrimonio informativo importante.

Ma questa facilità nell'accesso – straordinaria risorsa per i singoli e le istituzioni – è anche, paradossalmente, la più grande fonte di rischio delle pubblicazioni on-line, suscettibili di indicizzazione, riproduzione decontestualizzata, alterazione, e per questo in alcun modo assimilabili alle pubblicazioni cartacee.

Per questo, a legislazione vigente, abbiamo proposto la sottrazione delle sentenze dai motori di ricerca generalisti, così da coniugare il principio della pubblicità del processo – e del suo atto conclusivo – con la riservatezza dei soggetti a qualunque titolo coinvolti.

E dando, di una disciplina scritta 12 anni fa, un'interpretazione evolutiva, che tenga conto del quadro "costituzionale" europeo e delle differenze tra pubblicazione cartacea e telematica.

Si tratterebbe, oltretutto, di una soluzione analoga a quella utilizzata – anche su nostro impulso – proprio dalle Camere rispetto agli atti parlamentari, così da coniugare dignità individuale, pubblicità dei lavori e intangibilità degli atti parlamentari.

Ma oltre a deindicizzare le sentenze pubblicate integralmente, ci parrebbe più ragionevole favorire la massima conoscenza del patrimonio giuridico contenuto nelle sentenze, rendendole pubbliche il più possibile, ma oscurando i nomi presenti.

Si tratterebbe di una soluzione tanto più rilevante in un contesto, quale quello attuale, di progressiva telematizzazione del processo. In proposito, le garanzie suggerite nel tempo dal Garante al Governo, in sede di parere sui vari provvedimenti di disciplina del processo telematico, hanno consentito di fissare al punto più alto l'equilibrio tra trasparenza ed efficienza della giustizia da un lato e protezione dei dati personali, dall'altro.

Privacy, stampa e processi

Altrettanto importante per la qualità della nostra democrazia è il bilanciamento tra privacy e diritto all'informazione: tema su cui anche quest'anno non sono mancati interventi.

Importante, in particolare, la precisazione dei doveri di lealtà e correttezza cui il giornalista deve attenersi nell'esercizio della propria funzione, evitando soprattutto il ricorso ad artifici e raggiri o, perfino, come in un caso esaminato, alla sostituzione di persona.

Precisazione recentemente condivisa dall'Autorità giudiziaria in sede di impugnazione.

L'inchiesta giornalistica – che pure ha una funzione essenziale, da promuovere come straordinario strumento democratico – non può, infatti, ricorrere perfino a un atto che di per sé integra gli estremi di un reato, pur di carpire informazioni riservate e confidenziali.

Analogo esercizio di responsabilità è stato sollecitato in più occasioni, con riferimento alla cronaca giudiziaria e all'esigenza del rispetto del principio di essenzialità dell'informazione, infranto dalla divulgazione (spesso anche in violazione del regime di pubblicità degli atti investigativi sancito dal codice di rito) di ampi stralci o, addirittura, della versione integrale di atti d'indagine (interrogatori in carcere, intercettazioni), funzionali a soddisfare la curiosità del pubblico ma non reali esigenze informative rispetto al procedimento.

Il tutto con danno, spesso irreparabile, per i terzi – anche minori, talora vittime del reato – la cui esistenza viene in tal modo messa a nudo e riversata in rete, anche per sempre.

Abbiamo, quindi, adottato provvedimenti di blocco per impedire violazioni ulteriori in casi specifici di cronaca giudiziaria, sia riguardo ai terzi incolpevoli, sia rispetto a indagati di cui si è scandagliata sui giornali l'intera vita di relazione, senza alcuna connessione con le esigenze probatorie.

E abbiamo rappresentato al Governo la necessità di un riequilibrio nei

rapporti tra esigenze investigative, informazione e riservatezza, in un contesto di generale mediatizzazione della giustizia.

Il coinvolgimento a qualsiasi titolo in un procedimento non può, infatti, divenire la ragione, di per sé sufficiente, per esporre la parte o il terzo a una gogna che confonda il doveroso esercizio del diritto di cronaca con il sensazionalismo.

Auspichiamo pertanto che Parlamento e Governo vogliano farsi carico di quest'esigenza, coniugando gli aspetti della correttezza e lealtà dell'informazione e della riservatezza nelle indagini, nel rispetto del principio di proporzionalità tra privacy e mezzi investigativi ribadito, anche recentemente, dalla Corte di giustizia.

Diritto alla rete; diritti in rete

Quest'anno, in modo particolare, la rete è stata oggetto di un'attenzione crescente anche in sede parlamentare. Dalla Dichiarazione per i diritti in internet, ai disegni di legge costituzionale sull'accesso, alla disciplina del cyberbullismo e della tutela del minore, siamo stati partecipi di iniziative volte a sancire alcune minime garanzie per la dignità delle persone nell'Infosfera.

La rete costituisce una dimensione della vita entro cui si svolge – per citare l'art. 2 della Costituzione – la personalità di ciascuno.

Per questo e in questa misura, diviene un bene giuridico, meritevole di tutela soprattutto per non soccombere agli imperativi del mercato, per non rimettere a quella "legislazione privata" delle condizioni generali di contratto la garanzia, su scala mondiale, dei diritti fondamentali.

La sfida oggi, dunque, non è quella di giuridificare uno spazio che altrimenti, lasciato alla discrezionalità dell'etica individuale, troverebbe un suo ordine spontaneo: si tratta invece di difendere con determinazione la libertà di questo sterminato spazio pubblico.

Accanto alla straordinaria capacità di promuovere processi inclusivi, di partecipazione democratica e pluralistica, il web ha anche dimostrato – con

l'ambivalenza propria di ogni tecnologia – di poter amplificare, con effetti dirompenti, atti discriminatori, violenti, vessatori, spesso nei confronti dei soggetti più fragili o di quanti siano percepiti – e rappresentati – come diversi.

Dal *grooming* all'incitamento all'odio, alla violenza carnale – consumata off-line e poi esibita on-line, amplificandone così la potenza lesiva –; dalla "servitù volontaria" della prostituzione minorile, al cyberbullismo, nell'ampiezza delle sue accezioni.

Oltre al diritto alla rete, dunque, dobbiamo garantire, in rete, i diritti di tutti.

In primo luogo dei minori, vittime elettive di un uso distorto del web, perché non hanno gli strumenti per capire fino a che punto e con quali rischi esporre la propria vita, anche intima, agli altri.

La rete, paradossalmente, è il luogo in cui la fragilità dei minori emerge con maggior forza, in quello iato tra illusione di autonomia e introiezione di regole, esperienza della libertà ed esercizio di responsabilità.

La rete è anche il luogo in cui, nella presunzione di anonimato, minori violano altri minori.

E proprio questo è, forse, l'aspetto più tragico dell'uso violento della rete, in cui cioè l'autore e la vittima partecipano della stessa fragilità e della stessa inconsapevolezza del "risvolto" reale e concretissimo di ogni nostra azione nel digitale. Fenomeni che solo un esercizio consapevole del proprio diritto alla protezione dei dati personali e un nuovo codice etico della società digitale possono davvero contrastare.

È l'obiettivo che l'Autorità persegue ogni giorno, per far sì che la straordinaria "capacità generativa" della rete sia utilizzata non per violare, ma per promuovere i diritti di tutti.

L'Autorità: molti compiti, poche risorse

A fronte dei cambiamenti e degli scenari evocati, il Garante ha rafforzato e consolidato la propria attività.

Nel 2014 abbiamo adottato 628 provvedimenti collegiali, inclusi ricorsi e pareri resi al Governo. Sono 33.200 i quesiti ai quali l'Ufficio ha dato risposta, 577 sono state le sanzioni contestate, 385 le attività ispettive e di accertamento, svolte anche grazie all'ausilio della Guardia di Finanza, che unitamente al suo Comandante vogliamo ringraziare.

Un'attività intensa, anche a livello comunitario e internazionale, con la partecipazione ad oltre 80 riunioni, con importanti riconoscimenti per il lavoro svolto.

Siamo destinati a diventare parte integrante del sistema europeo dove il nuovo Regolamento ci affida compiti ancora più impegnativi e spinge verso modelli stringenti di collaborazione e condivisione con le altre Autorità.

Per questo, il ruolo del Garante deve essere rafforzato con mezzi e risorse adeguate, come richiesto dalla recente Conferenza di Manchester.

Ho rappresentato da tempo al Governo e al Parlamento l'urgenza di una seria revisione dell'attuale anacronistico sistema di finanziamento, non più sostenibile e tale da mettere fortemente a rischio, fino a precluderla del tutto, la nostra attività: in evidente contrasto con quanto imposto agli Stati membri dai Trattati.

Rinnoviamo la sollecitazione per una risposta non elusiva.

Prima di concludere, consentitemi di ringraziare le Colleghe Augusta Iannini, Licia Califano, Giovanna Bianchi Clerici che con me compongono il Collegio del Garante, con le quali condivido quotidianamente responsabilità e decisioni.

Desidero altresì ringraziare il Segretario generale Giuseppe Busia e coloro che nell'Ufficio, ogni giorno, lavorano con generosità e competenza per dare risposta alle crescenti domande di tutela dei cittadini.

In evidenza – 2014

Gennaio

A seguito di accertamenti avviati d'ufficio, abbiamo vietato l'uso dei dati personali riferiti a pazienti con insufficienza renale cronica da parte di un'associazione di medici nefrologi che gestisce un importante registro nazionale finalizzato allo svolgimento di analisi statistiche ed epidemiologiche (dati trasferiti anche in un analogo registro privato europeo), prescrivendo in pari tempo – al fine di soddisfare esigenze di ricerca medico-scientifica ritenute meritevoli – l'adozione di misure di sicurezza e di accorgimenti, ulteriori rispetto a quelli esistenti, volti ad assicurare l'anonimato degli interessati e ad informare gli stessi circa tale impiego ulteriore dei dati raccolti dalle strutture pubbliche di dialisi [par. 8.1]

Nel rispondere ad un quesito posto dalla Presidenza del Consiglio - Dipartimento per la funzione pubblica relativo alla legittimità di pubblicazione sul proprio sito web istituzionale dei nominativi dei fruitori di permessi sindacali, abbiamo affermato che, in base al d.lgs n. 33/2013 e al Codice, detti soggetti non rientrano tra coloro per i quali è prevista tale forma di pubblicità e che, al fine di soddisfare l'esigenza di trasparenza, è comunque possibile la pubblicazione in forma aggregata di tali informazioni [par. 13.3]

Abbiamo autorizzato un'azienda ospedaliero-universitaria a trattare i dati sanitari e genetici di circa duecento pazienti nell'ambito di uno studio monocentrico, approvato dal competente comitato etico, volto a monitorare gli esiti clinici di malati con cirrosi epatica sottoposti a trapianto di fegato nell'arco di cinque anni (con riguardo anche ai dati e ai campioni dei pazienti deceduti nel periodo successivo al trapianto, salvo che non si siano opposti in vita all'uso dei dati a scopo di ricerca), dopo aver informato e raccolto il consenso dei pazienti in vita [par. 7]

Parere favorevole è stato reso in merito allo schema di regolamento che definisce le modalità di funzionamento e collegamento della Banca nazionale unica della documentazione antimafia con il Ced interforze del Dipartimento della pubblica sicurezza ed altre banche dati. L'archivio, cui potranno accedere i soggetti che possiedono specifici profili di autorizzazione, consentirà di semplificare il sistema di rilascio della documentazione antimafia sulle imprese (cd. "comunicazioni" e "informazioni" antimafia) alle stazioni appaltanti e agli altri soggetti legittimati ad acquisirle (pubbliche amministrazioni, camere di commercio, ordini professionali ecc.) [parr. 9.2 e 3.4.1]

È stato reso un parere favorevole sullo schema di decreto del Ministero del lavoro relativo alla costituzione presso l'Inps del Casellario dell'assistenza, vale a dire l'anagrafe generale delle posizioni assistenziali, che ha accolto i suggerimenti forniti dall'Autorità (concernenti principalmente la selezione delle informazioni destinate a confluire nel casellario, l'individuazione dei soggetti che possono consultarle, le modalità di raccolta e di anonimizzazione dei dati relativi ai minori in situazioni di disagio) [parr. 4.2 e 3.4.1]

Febbraio

Alla luce delle mutate condizioni del mercato delle comunicazioni e della *number portability*, abbiamo aggiornato le prescrizioni impartite con il provvedimento generale del 25 giugno 2009 alle società telefoniche che svolgono attività di profilazione, permettendo l'analisi di alcune tipologie di dati della clientela in forma aggregata nell'intervallo temporale di due giorni [par. 12.4]

Visti gli esiti della consultazione pubblica, è stato adottato un provvedimento generale che impone agli operatori di *telemarketing* di adottare specifiche misure per ridurre drasticamente il fenomeno delle cd. "telefonate mute" [par. 12.2]

Marzo

È stata avviata una consultazione pubblica su uno schema di provvedimento relativo all'eventuale costituzione di una banca dati interoperatore dei clienti morosi nell'ambito dei servizi di comunicazione elettronica denominata Sit [par. 14.3]

Abbiamo dichiarato illecito e bloccato il trattamento dei dati effettuato da un ente pubblico mediante la diffusione sul proprio sito web istituzionale delle graduatorie (intermedia e definitiva) di un concorso riservato a disabili contenente dati idonei a rilevare lo stato di salute di oltre 500 concorrenti [par. 13.3]

Abbiamo fissato un quadro organico di regole per la tutela della riservatezza nel delicato ambito del trattamento dei dati da parte dei partiti politici in relazione agli aderenti e a quanti hanno contatti regolari nonché in relazione a simpatizzanti e partecipanti a singole iniziative (petizioni, proposte di legge, richieste di *referendum*). In un'ottica di semplificazione e contemperamento degli interessi, abbiamo esonerato in via definitiva partiti, movimenti, comitati e singoli candidati che fanno propaganda elettorale utilizzando alcune fonti pubbliche liberamente utilizzabili a tale scopo (ad es. le liste elettorali) dall'obbligo di rendere l'informativa dal sessantesimo giorno precedente la data delle consultazioni politiche, amministrative, referendarie o delle "primarie" al sessantesimo giorno successivo alla loro conclusione [par. 4.5]

Aprile

Su richiesta degli operatori di settore e considerati i mutamenti normativi e tecnologici, è stato promosso l'aggiornamento del codice di deontologia e buona condotta dei sistemi di informazione creditizia (sic) costituiti per verificare l'affidabilità, la puntualità nei pagamenti e il rischio di sovraindebitamento di quanti intendono accedere al credito al consumo [par. 14.2]

Abbiamo reso parere favorevole su uno schema di decreto del Presidente del Consiglio dei ministri in materia di destinazione del due per mille dell'irpef a favore di partiti politici, in base alla scelta del contribuente, evidenziando la necessità di una più puntuale definizione delle misure a tutela della riservatezza circa le determinazioni individuali, nonché, nella stessa materia, sullo schema di provvedimento del Direttore dell'Agenzia delle entrate con il quale è stata definita la scheda da utilizzare, in via transitoria, nell'esercizio finanziario 2014 per effettuare tale scelta [par. 2.1.1]

Abbiamo condizionato il parere favorevole reso su uno schema di regolamento del Ministero dell'Interno che individua le modalità di attuazione e di funzionamento dell'Anagrafe nazionale della popolazione residente (Anpr) all'introduzione di una serie di misure ed accorgimenti, quali l'individuazione dei soggetti cui sono rimessi i controlli, il divieto di duplicazione delle anagrafi, la consultazione dell'Autorità sulla definizione di *standard* di qualità dei dati e l'adozione di elevate misure di sicurezza [parr. 4.5 e 3.4.1]

Maggio

Allo scopo di contemperare le esigenze di pubblicità e trasparenza con i diritti e le libertà fondamentali nonché la dignità delle persone, abbiamo individuato in apposite Linee guida cautele e misure da adottare quando sono diffusi sul web dati personali per finalità di trasparenza amministrativa in base al decreto legislativo n. 33/2013. Si è inoltre chiarito che i dati così pubblicati non sono liberamente utilizzabili da chiunque per qualunque finalità, ma solo in termini compatibili con gli scopi per i quali sono raccolti [par. 4.4]

Con provvedimento di carattere generale, abbiamo individuato modalità semplificate per rendere l'informativa *online* sui trattamenti effettuati mediante *cookie*: all'utente deve essere chiaramente ed immediatamen-

te rappresentato se il sito utilizza *cookie* di profilazione per inviare messaggi pubblicitari mirati o se il sito consente anche l'invio di *cookie* di "terze parti" (ossia di *cookie* installati da un sito diverso tramite il sito che si sta visitando). Deve essere assicurato un *link* a un'informativa più ampia sull'utilizzo dei *cookie* e la possibilità di negare il consenso alla loro installazione [par. 11.5]

Anche tenendo conto delle indicazioni pervenute in sede di consultazione pubblica, abbiamo impartito prescrizioni ai titolari che effettuano trattamenti dati in ambito *mobile payment* utilizzando *smartphone*, *tablet* e pc [par. 12.6]

A seguito dello *Sweep Day* dedicato al controllo di *app* per *smartphone* e *tablet*, le Autorità che hanno partecipato all'iniziativa, e tra queste il Garante, hanno reso pubblica la lettera congiunta indirizzata alle maggiori piattaforme e agli operatori del mercato delle *app*, evidenziando i numerosi casi di *app* prive di qualsiasi *privacy policy* [par. 23.5]

È stato espresso parere favorevole su uno schema di decreto del Presidente del Consiglio dei ministri che consentirà a Regioni e Province autonome di dare il via al fascicolo sanitario elettronico (Fse) con il quale si individuano i primi contenuti da attivare a livello nazionale (l'informativa da rendere ai pazienti; i dati e i documenti da inserire, con opzioni rimesse alla volontà individuale; le responsabilità e i compiti dei soggetti coinvolti; le garanzie e le misure di sicurezza da adottare nel trattamento dei dati personali; le modalità e i livelli diversificati di accesso al fascicolo; i criteri di interoperabilità nonché i contenuti informativi e le codifiche del profilo sanitario sintetico e del referto di laboratorio) [parr. 6.1.2 e 3.4.1]

Abbiamo dato notizia al Presidente del Consiglio dei ministri delle rilevanti criticità emerse nel corso di una serie di ispezioni presso gli *Internet eXchange Point* (Ixp) nazionali – presso i quali si interconnettono le infrastrutture di rete dei maggiori operatori di tlc nazionali e internazionali, degli *Internet service provider*, nonché di importanti fornitori di servizi *online* e che, tra l'altro, ospitano gli apparati che gestiscono le reti di comunicazione tra quasi tutte le pubbliche amministrazioni italiane nonché quelle degli enti di ricerca – al fine di consentirne la tempestiva valutazione da parte degli organismi preposti alla sicurezza cibernetica del Paese [par. 22.3]

Abbiamo accolto la richiesta di verifica preliminare presentata dalla Banca d'Italia relativa all'uso di sistemi di videosorveglianza "intelligente" in relazione agli specifici rischi connessi allo stoccaggio e alla gestione di elevate quantità di valori [par. 4.8]

Giugno

Abbiamo reso il parere su uno schema di decreto del Presidente del Consiglio dei ministri recante la definizione delle caratteristiche del Sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (Spid) – Sistema volto, nel suo complesso, a favorire la diffusione di servizi in rete mediante l'attribuzione a ciascun soggetto interessato di un'"identità digitale" – nonché dei tempi e delle modalità di sua adozione da parte di pubbliche amministrazioni e imprese [parr. 4.2 e 3.4.1]

È stato aggiornato il codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e di ricerca scientifica effettuati nell'ambito del sistema statistico nazionale (All. A3 al Codice) [par. 8.2]

Luglio

Dopo aver seguito fin dall'inizio (2012) il negoziato in seno al Gruppo di lavoro del Consiglio UE (DAPIX) incaricato di licenziare le modifiche alle proposte di Regolamento e di Direttiva in materia di protezione dei dati personali, abbiamo rafforzato la collaborazione con il Governo in occasione del

semestre di Presidenza italiana dell'UE nel corso del quale si è raggiunto un accordo fra gli Stati Membri su punti essenziali della Proposta di Regolamento (trasferimento di dati verso Paesi terzi, obblighi di responsabili e incaricati del trattamento, trattamenti per finalità di pubblico interesse) e si è fatta maggiore chiarezza sul campo di applicazione della Proposta di Direttiva concernente le attività giudiziarie e di polizia [par. 23.1]

Abbiamo disposto il blocco rispetto alla diffusione da parte di alcune testate delle trascrizioni delle intercettazioni telefoniche riguardanti la vicenda di un fotografo accusato di reati sessuali nei confronti di minorenni, non rispettosa dei limiti del diritto di cronaca e dell'essenzialità dell'informazione [par. 10.1]

Abbiamo prescritto a Google di adottare un'informativa per gli utenti strutturata su più livelli e di acquisire il previo consenso degli stessi – ancorché con modalità semplificate – in caso di utilizzo dei dati a fini di profilazione e pubblicità comportamentale personalizzata; dovranno essere altresì definiti tempi certi di conservazione dei dati (conservati sui sistemi cd. "attivi" ovvero di *back up*) [par. 11.2]

Abbiamo negato l'autorizzazione all'installazione di un sistema di videosorveglianza all'interno degli spogliatoi dei dipendenti considerate le caratteristiche invasive dello stesso su riservatezza e dignità degli interessati (nonché considerata la sua scarsa utilità nel contrasto di furti comunque avvenuti in altri locali aziendali) [par. 13.1]

Anche alla luce delle Linee guida del Garante del 2009, in più occasioni siamo intervenuti presso aziende sanitarie e strutture ospedaliere per assicurare la correttezza nelle fasi di realizzazione e successivo utilizzo dei *dossier* sanitari elettronici, prescrivendo misure per la tenuta dei dati personali, e idonei accorgimenti, anche tecnici, per selezionare l'accesso agli stessi nonché per consentire all'interessato di ottenere l'oscuramento di singoli eventi clinici [par. 6.1.2]

Abbiamo reso parere favorevole sul sistema di ripresa delle immagini avviato in via sperimentale dal Dipartimento della pubblica sicurezza in quattro città mediante microtelecamere indossabili dagli agenti di polizia nel corso di manifestazioni pubbliche ed attivabili solo in caso di criticità, con l'indicazione di misure sulla tenuta delle schede video nonché su modalità e tempi di conservazione dei dati registrati [par. 9.2]

Abbiamo reso un parere favorevole sulle modifiche apportate dal Coni al proprio regolamento per il trattamento dei dati sensibili e giudiziari, con particolare riferimento ai trattamenti di dati che riguardano un gruppo selezionato di atleti (inseriti nel *registered testing pool* nazionale) effettuati attraverso l'*Anti-Doping Administration & Management System* (ADAMS), rispetto ai quali il Coni potrà effettuare, ove necessario, operazioni di trasferimento all'estero, verso la banca dati ADAMS e verso le organizzazioni *anti-doping* ubicate anche in Paesi terzi di volta in volta competenti a testare gli atleti [par. 4.1]

Abbiamo reso parere favorevole – con riserve rispetto al previsto scambio di dati sul dna verso Paesi terzi – sullo schema di regolamento, attuativo della legge 30 giugno 2009, n. 85, in materia di banca dati nazionale del dna e laboratorio centrale per la banca dati nazionale del dna [parr. 9.2 e 3.4.1]

Settembre

Abbiamo ritenuto illecita l'acquisizione e la diffusione radiofonica della registrazione del contenuto di una comunicazione telefonica intercorsa con un esponente politico ed effettuata da parte di un giornalista utilizzando, in violazione del principio di correttezza, un "artificio" (segnatamente, l'imitazione della voce di un altro esponente politico amico dell'interessato) [par. 10.3]

Abbiamo ritenuto ammissibile il trattamento di dati personali effettuato attraverso la localizzazione di dispositivi *smartphone* forniti ai dipendenti per finalità organizzative e di sicurezza sul lavoro, nel rispetto dell'art. 4 dello Statuto dei lavoratori, purché non vengano trattati altri dati (sms, telefonate) e siano adottate opportune misure di sicurezza [par. 13.1]

Ottobre

Abbiamo vietato ad una società di intermediazione di prestiti *online* l'utilizzo dei dati personali degli utenti forniti nella richiesta di preventivo per la diversa finalità di *marketing* in assenza di un consenso liberamente prestato a tal fine [par. 11.3]

A seguito di consultazione pubblica, abbiamo adottato un provvedimento generale (con le allegate Linee guida) in materia di dati biometrici grazie al quale, nel rispetto del principio di minimizzazione e con l'individuazione di numerose misure di sicurezza, sono state identificate alcune tipologie di trattamento che, per le finalità perseguite, presentano un livello ridotto di rischio e non necessitano della verifica preliminare da parte dell'Autorità, in particolare in relazione a forme di autenticazione informatica, per il controllo di accesso fisico ad aree "sensibili" (ad es. destinate all'utilizzo di apparati e macchinari pericolosi), per la sottoscrizione di documenti informatici nonché per scopi cd. facilitativi [par. 15.2]

Novembre

Abbiamo stabilito che le strutture sanitarie non possano raccogliere in maniera sistematica e preventiva informazioni sulle convinzioni religiose dei pazienti e, più in generale, quando ciò non sia indispensabile [par. 6.1]

Abbiamo adottato i primi provvedimenti dopo la sentenza della Corte di giustizia nel caso "Google Spain" relativi alle richieste di cancellazione dai risultati dei motori di ricerca in Internet dei collegamenti alle pagine web che contengono il nominativo dell'interessato [par. 10.4]

Abbiamo reso parere favorevole su uno schema di provvedimento del Ministero del lavoro concernente il modello di Dichiarazione sostitutiva unica (Dsu) necessario per il calcolo dell'Isee, lo strumento di valutazione della situazione economica di coloro che richiedono prestazioni sociali agevolate. Gli interessati dovranno essere informati in modo chiaro sull'uso che viene fatto dei loro dati (finalità, tempi di conservazione, ambito di comunicazione) mediante apposita informativa inserita nella parte iniziale della dichiarazione (dalla quale dovrà altresì risultare che i controlli dell'Inps sulle informazioni fornite dal dichiarante si estenderanno anche a dati personali dei componenti il nucleo familiare, quali la situazione reddituale e patrimoniale) [parr. 4.2 e 3.4.1]

Dicembre

Abbiamo rinnovato le autorizzazioni generali per il trattamento di dati sensibili e giudiziari [par. 1]

Nel parere reso all'Istituto nazionale della previdenza sociale (Inps) avente ad oggetto uno schema di convenzione tra l'Istituto e Confindustria, Cgil, Cisl e Uil (prevista dal "Testo unico sulla rappresentanza" sottoscritta il 10 gennaio 2014), abbiamo evidenziato che per misurare la rappresentatività sindacale nel settore privato ai fini della contrattazione nazionale di categoria non è necessaria la trasmissione da parte delle imprese all'Inps dei dati concernenti l'affiliazione sindacale di ciascun lavoratore, potendosi perseguire lo stesso fine mediante la sola rilevazione del numero di deleghe assegnate a ciascuna sigla sindacale [par. 13]

I – Stato di attuazione del Codice in materia di protezione dei dati personali

1 Introduzione: i principali interventi dell'Autorità nel 2014

1.1. Se la materia della protezione dei dati personali trascende i confini nazionali (e fin dalle origini aspira ad estendersi su scala globale), non pare revocabile in dubbio che nel 2014 questa vocazione naturale si sia pienamente manifestata, sia in relazione ai passi avanti fatti nell'opera di ammodernamento del quadro normativo di riferimento (nell'ambito dell'Unione europea come pure del Consiglio d'Europa), sia per la significatività (e gli effetti) delle sentenze pronunciate dalla Corte di giustizia dell'Unione europea.

Entrambi gli sviluppi cui si è appena fatto cenno non sono rimasti senza effetti sull'attività dell'Autorità, che da sempre si caratterizza per dinamismo nell'ambito del Gruppo dei Garanti europei istituito dall'art. 29 della direttiva 95/46/CE – del quale, a novembre, il Presidente dell'Autorità è stato eletto vicepresidente – e sui diversi tavoli internazionali nei quali è chiamata ad operare (cfr. par. 23 e, per un quadro di sintesi, i dati riepilogativi riportati nella sez. IV, tab. 25).

Dopo aver seguito fin dalle prime battute il negoziato in seno al Gruppo di lavoro del Consiglio UE (DAPIX), nell'ambito del processo legislativo che dovrebbe portare all'adozione delle Proposte di Regolamento e di Direttiva in materia di protezione dei dati personali, l'Autorità ha rafforzato la collaborazione con il Governo in occasione del semestre di Presidenza italiana dell'UE, arco temporale nel corso del quale si è raggiunto un accordo fra gli Stati membri su alcuni elementi essenziali della Proposta di Regolamento (trasferimento di dati verso Paesi terzi, obblighi di titolari e responsabili del trattamento, trattamenti per finalità di pubblico interesse) e si è fatta maggiore chiarezza sul campo di applicazione della Proposta di Direttiva concernente le attività giudiziarie e di polizia (par. 23.1).

L'Autorità ha operato attivamente anche nell'ambito del Comitato intergovernativo incaricato dal Comitato dei ministri di portare a termine il processo di modernizzazione della Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale n. 108/1981 del Consiglio d'Europa, conclusosi con l'adozione, nel dicembre 2014, del documento contenente la Convenzione modernizzata che attende ora la definitiva approvazione del Comitato dei ministri (par. 23.5).

1.2. Si è già fatto cenno alle sentenze pronunciate dalla Corte di giustizia, i cui assunti potranno riverberare nella più ampia discussione del *legal framework* europeo,

ma i cui effetti già in parte si registrano nell'ordinamento nazionale: ciò vale per la definizione dell'(ampio) ambito di applicazione della direttiva 95/46/CE (e quindi delle discipline nazionali di recepimento), sia con riguardo all'utilizzo di sistemi di videosorveglianza per finalità personali – quando in grado di riprendere aree pubbliche ancorché posti a presidio del domicilio da parte di privati (11 dicembre 2014, František Ryneš c. Úřad pro ochranu osobních údajů, causa C-212/13: par. 14.5) –, sia in relazione a soggetti stabiliti in Paesi terzi, segnatamente Google, società ritenuta titolare del trattamento concernente i dati personali pubblicati *online* da terzi e rinvenibili utilizzando le funzionalità del motore di ricerca (13 maggio 2014, C-131-12, Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos e Mario Costeja González: cfr. par. 10.4).

Invece, non solo è rimasta senza effetti nell'ordinamento nazionale – segnatamente rispetto alla disciplina contenuta nell'art. 132 del Codice – la sentenza (già segnalata nella Relazione 2013) dell'8 aprile 2014 (Digital Rights Ireland e Seitlinger e a., cause riunite C-293/12 e C-594/12), con la quale la Corte di giustizia ha dichiarato invalida la direttiva sulla conservazione dei dati di traffico, ritenendo che dalla stessa derivi un'ingerenza di ampia portata e di particolare gravità nei diritti fondamentali al rispetto della vita privata e alla protezione dei dati, ma anzi il Garante ha dovuto nuovamente richiamarne i contenuti in occasione delle misure (ulteriormente invasive) introdotte in sede di conversione del decreto-legge 18 febbraio 2015, n. 7, la cui portata, in particolare all'art. 4-*bis*, è stata solo in parte attenuata nel testo definitivo della legge di conversione 17 aprile 2015, n. 43 (cfr. doc. web n. 3807700).

Non può trascurarsi, infine, la circostanza che la Corte sia tornata a pronunciarsi, per la terza volta, sul tema dell'indipendenza delle autorità di protezione dei dati personali (8 aprile 2014, Commissione c. Ungheria, causa C-288/12), carattere irrinunciabile nell'architettura costituzionale europea risultante dal disegno tracciato dalla Carta dei diritti fondamentali dell'Unione europea (art. 8) e dai Trattati (artt. 16 TFUE e 39 TUE).

1.3. Ma l'impegno dell'Autorità, pur catalizzato dal processo di cambiamento in essere presso le Istituzioni sovranazionali in ragione delle sue ricadute sull'ordinamento interno, non si è limitato a (e tanto meno esaurito in) quanto accade oltreconfine (per uno sguardo d'insieme, v. i dati statistici riportati nella sez. IV, tab. 1). Costante e fattivo è infatti il rapporto collaborativo consolidatosi negli anni con il Governo e le singole Amministrazioni del quale sono visibili i frutti, anzitutto nei pareri resi (scanditi nel par. 3.4), in relazione ai quali, diversamente da quanto accaduto negli anni precedenti, non si sono registrati casi di mancata consultazione del Garante. Dall'esame del loro contenuto si desume che il Garante è chiamato a pronunciarsi (a volte con una tempistica serrata) nelle materie più disparate, sempre più spesso soffermandosi anche su complessi profili tecnologici.

Gli ambiti toccati riguardano i principali progetti di modernizzazione del Paese – quali il Sistema pubblico per la gestione dell'identità digitale di cittadini ed imprese (Spid) (par. 4.2) o l'Anagrafe nazionale della popolazione residente (Anpr) (par. 4.5) –, i sistemi informativi preordinati ad incrementare l'efficienza dell'azione amministrativa – si pensi al Casellario dell'assistenza (par. 4.2), al Sistema informativo nazionale per la prevenzione nei luoghi di lavoro (Sinp) (par. 4.2) o alla Banca nazionale unica della documentazione antimafia (par. 9.2) – e, ancora, gli archivi orientati ad un più efficace contrasto ai fenomeni criminali nel rispetto dei diritti fondamentali degli interessati, come nel caso della progettata banca dati nazionale del dna (par. 9.2).

Attenzione è stata anche posta, in attesa del completamento del faticoso processo che dovrebbe condurre all'adozione della direttiva per i trattamenti effettuati per