GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Big data
e sorveglianza globale

Discorso del Presidente

Antonello Soro

Relazione2013

www.garanteprivacy.it

Relazione2013

Discorso del Presidente

Antonello Soro

Roma, 10 giugno 2014

Signor Presidente del Senato,

Autorità, Signore e Signori,

É trascorso un anno particolarmente importante per la nostra Autorità: il diritto alla protezione dei dati personali è stato al centro di molte attenzioni da parte delle Istituzioni e, soprattutto, dell'opinione pubblica.

Le vicende internazionali sullo spionaggio informatico e l'indignazione che ne è seguita hanno rappresentato l'occasione per una grande nuova consapevolezza dei diritti ma, insieme, un elemento di rottura che ha aperto molte dispute sul terreno giuridico, politico, nei rapporti tra Stati e ha seriamente compromesso la fiducia dei cittadini per le innovazioni legate alla rivoluzione digitale.

Le rivelazioni di Edward Snowden hanno rilanciato l'esigenza di porre la tutela dei dati a fondamento dello statuto di cittadinanza, perché in un mondo segnato dall'incontenibile affidamento alla tecnologia di parti essenziali della nostra esistenza, proteggere i nostri dati significa proteggere la nostra vita e la nostra libertà.

L'idea di *privacy*, nella sua più compiuta accezione, rappresenta uno straordinario segnalatore dell'organizzazione sociale, giuridica, valoriale del nostro tempo, attraverso cui è possibile cogliere tendenze e contraddizioni, potenzialità e rischi, intravvedere orizzonti, assumere decisioni più consapevoli.

Il diritto alla riservatezza, tradizionalmente inteso come diritto a tutelare la vita intima dalle diverse ingerenze, ha assunto, nel mondo nuovo pervaso e condizionato dalle tecnologie, un profilo sempre più connesso alla dignità della persona, quale sintesi delle libertà che ci appartengono: libertà di scegliere, di non essere omologati, di non essere controllati, di esprimere spontaneamente la nostra creatività.

I cambiamenti imposti dall'evoluzione incessante delle tecnologie accompagnano tutti gli aspetti della nostra quotidianità e pongono sfide rilevanti per l'Autorità.

E proprio perché Istituzione preposta alla tutela di un diritto - riconosciuto come fondamentale dall'ordinamento europeo - la funzione di garanzia che siamo chiamati a svolgere ha un ruolo centrale nella moderna società per assicurare il necessario equilibrio tra autorità e libertà, vita privata e informazione, *privacy* e sicurezza, persona e mercato, riservatezza e trasparenza.

In una cornice di profondi mutamenti, in ragione anche degli effetti globali dei fenomeni e dei limiti geografici in cui operiamo, avvertiamo quanto sia difficile rafforzare le garanzie per i cittadini, rendere più efficaci le tutele, imporre regole a soggetti economici di dimensioni planetarie.

Se è vero che l'equilibrio tra tecnologie e tutela dei diritti fondamentali nello spazio digitale deve trovare un'efficace risposta ultrastatuale (importante in questo senso è la Risoluzione del novembre 2013 dell'Assemblea generale delle Nazioni Unite), è altrettanto vero che quanti hanno responsabilità e poteri hanno anche il dovere di mettere in campo impegno e determinazione per contrastare le distorsioni del sistema.

Per questo non si può tacere la delusione per la scarsa risolutezza manifestata dai Governi nell'approvazione del nuovo Regolamento europeo in materia di protezione dei dati, occasione perduta per dotarsi di un solido quadro legislativo capace di rappresentare un ineludibile punto di riferimento globale.

Auspichiamo con forza che l'imminente presidenza italiana del Consiglio dell'Unione possa essere l'occasione per ridare impulso al progetto.

Proprio perché centrale in una democrazia che voglia essere davvero liberale e riconoscere la persona come asse portante della sua

architettura, il diritto alla protezione dati deve essere un riferimento costante nell'attività legislativa.

Privacy e sicurezza

Il *Datagate* ha rappresentato un punto di non ritorno nel rapporto tra *privacy* e sicurezza.

Quasi specularmente opposto a quell'11 settembre, che così profondamente aveva mutato la percezione delle nuove minacce, inducendo tolleranza per crescenti limitazioni della libertà in nome di un'idea, rassicurante sebbene illusoria, della sicurezza.

Le rivelazioni su *Prism* hanno dimostrato quanto possa essere rischiosa per la democrazia la combinazione in un unico Paese, ancorché democratico, tra concentrazione dei principali *provider* e leggi emergenziali contro il terrorismo.

Rischi, questi, ulteriormente aggravati dalla vulnerabilità dei sistemi informatici cui sono affidati, assieme alle comunicazioni, interi pezzi della vita di ciascuno, resi accessibili alle agenzie d'*intelligence* da norme ispirate alla logica autoritaria dell'"uomo di vetro", secondo cui chi non ha nulla da nascondere non ha neanche nulla da temere.

Del resto, da sempre i regimi autoritari - e molti ve ne sono ancora nel mondo - hanno fatto dell'intrusione "nelle vite degli altri" il principale strumento di potere: per questo difendere la *privacy* significa anzitutto difendere la libertà.

Lo ha ben chiarito la Corte di giustizia, che lo scorso 8 aprile ha dichiarato illegittima la direttiva sulla *data retention* per violazione del principio di proporzionalità nel bilanciamento tra *privacy* e sicurezza, che si dovrebbe concretizzare attraverso un valutazione del tipo di reato e delle esigenze investigative, con il vaglio di un'autorità terza, magistratuale o amministrativa indipendente.

È importante che verso questo approccio, tipicamente europeo, si stia orientando anche il Congresso degli Stati Uniti.

La protezione dei dati presuppone necessariamente la protezione dei sistemi che tali dati conservano.

Tanto più con riferimento a banche dati strategiche per quantità e qualità del loro contenuto quali, in particolare, quelle gestite dal Ministero dell'interno per esigenze di sicurezza (dalla banca dati antimafia al CED della Polizia), per le quali l'Autorità ha promosso più elevati livelli di garanzia - nell'interesse dei cittadini i cui dati sono trattati e delle stesse esigenze investigative - che dovranno essere estesi anche alla nuova banca dati del DNA.

Privacy e sicurezza pubblica sono complementari non solo perché la prima riduce la vulnerabilità di sistemi e infrastrutture funzionali alla seconda, ma anche perché una massiva acquisizione di dati non garantisce indagini più efficaci e equilibrate, per le difficoltà correlate alla gestione di un patrimonio informativo per nulla selettivo.

La minaccia cibernetica costituisce oggi la sfida più temibile per gli Stati.

Una strategia di difesa davvero efficace presuppone allora un'adeguata selezione degli obiettivi da controllare e dei dati da acquisire, nonché l'adozione di cautele utili a garantire la sicurezza dei sistemi.

Ci siamo impegnati per assicurare la nostra funzione - come prevede il Codice - anche nel contesto dell'*intelligence*, tradizionalmente caratterizzato dalla recessività dei diritti individuali rispetto alle esigenze di sicurezza nazionale. Soprattutto alla luce dell'attribuzione ai Servizi di specifiche competenze in questa materia e, dunque, del contestuale ampliamento dei loro poteri di accesso sistematico a tutti i *database* pubblici e privati, anche ai sensi del d.P.C.M. 24 gennaio 2013.

Il Garante ha siglato con il DIS un protocollo d'intesa per acquisire

alcuni elementi informativi su questi specifici trattamenti, che proprio per la loro potenziale invasività richiedono adeguate garanzie che spetta anche alle Autorità di protezione dati assicurare (come ribadito dalla Corte costituzionale tedesca, sent. n. 31/2013).

Il protocollo - che non ha precedenti in Europa - è un fatto in sé molto importante.

Vorremmo che rappresentasse la "cifra" della politica di sicurezza del Governo, di qui in avanti.

Esigenze analoghe di protezione dati fondano il provvedimento destinato alle Procure della Repubblica e riferito alle attività di intercettazione, con cui il Garante, senza minimamente incidere su profili inerenti l'esercizio della giurisdizione, ha prescritto misure essenziali per la riservatezza dei cittadini a vario titolo intercettati. Su questa scelta abbiamo registrato qualche incomprensione: ma pensiamo che non sia più rinviabile, da parte di tutte le Istituzioni coinvolte, un supplemento di responsabilità.

La società digitale: dalla persona ai dati

La missione che siamo chiamati a svolgere e le sfide ambiziose che dobbiamo affrontare non possono prescindere dalla consapevolezza delle modifiche strutturali e radicali intervenute negli stili di vita, nell'organizzazione del lavoro, nei processi economici, nella modernizzazione della pubblica amministrazione: ogni nostra relazione si basa su una raccolta continua e inarrestabile di informazioni.

Dai comportamenti in Rete (pagine visitate, tempi di lettura, informazioni condivise), ai dati raccolti dalle varie applicazioni (percorsi più veloci, funzioni vitali del nostro corpo, posizione geografica) o contenute nei nostri *account* di posta elettronica, ai sensori intelligenti che captano anche gli stati d'animo, tutto ruota intorno alla profilazione,

sempre più individualizzata e pervasiva, le cui tecniche sono in grado di elaborare raffinate identità digitali con modalità e rapidità fino ad oggi impensabili.

L'integrazione tecnologica e la connettività permanente ampliano a dismisura la possibilità di raccogliere, archiviare, elaborare informazioni e consentono, superando i limiti di tempo e di spazio, di aggregare un'enorme quantità di dati a costi contenuti (si pensi alle potenzialità offerte dal *Cloud*).

Siamo perennemente connessi e siamo disposti, spesso inconsapevolmente, a consegnare informazioni in cambio di vantaggi o comodità. Quasi attoniti davanti alla "grande fiera delle meraviglie" dei prodotti digitali.

Quelle cedute però non sono soltanto le nostre generalità, ma la radiografia completa di interessi, opinioni, consumi, spostamenti, in sostanza pezzi della nostra vita che come tessere di un mosaico si scompongono e ricompongono per formare il nostro profilo identitario.

Lo spazio digitale non è una realtà parallela, ma la dimensione in cui si dispiega una parte sempre più importante della vita reale. Ogni gesto quotidiano lascia tracce digitali che nessuno potrà far scomparire.

La rappresentazione della nostra persona è sempre più affidata ad informazioni frammentate e sparse in banche dati la cui collocazione è spesso ignota.

Anche la relazione tra potere pubblico e persona si basa sempre più su una raccolta incessante di dati, di qualsiasi informazione riguardi l'individuo e le sue relazioni, sulla funzione demiurgica dell'algoritmo.

L'algoritmo classifica, incrocia, elabora, costruisce profili, archivia e indicizza le persone come astrazioni inconsapevoli, sospese in una dimensione immateriale e incapaci di essere appunto libere.

La persona digitale, dematerializzata, disincarnata, è destinata

a coincidere soltanto con le informazioni che la riguardano, che altri soggetti scelgono di selezionare, trattare e rivelare attraverso i motori di ricerca.

In questo modo quelle informazioni diventano l'unica proiezione nel mondo dell'essere di ciascuno, non un doppio virtuale che si affianca alla persona reale ma rappresentazione istantanea di un'intera vita, unica memoria sociale di quella vita e, come tale, capace di condizionare la memoria individuale, di orientare relazioni e destini di ciascuno. Durante la vita e dopo la morte.

La sorveglianza nel tempo dei *Big data*

La delicatezza dei dati raccolti e archiviati in giganteschi *server* e la capacità di analizzare comportamenti individuali e collettivi elaborando miliardi di informazioni è tanto più evidente se si riflette sull'intreccio pericoloso, che il *Datagate* ha soltanto portato alla luce, e che può realizzarsi ogni giorno, tra aziende digitali e spionaggio. I dati collezionati per finalità commerciali diventano sempre più interessanti anche per fini di sicurezza, a cui sono ormai irreversibilmente intrecciati.

Ancora più delicato è il potere che si concentra nelle mani delle grandi aziende che dispongono di un patrimonio informativo immenso e poggiano le loro attività quasi esclusivamente sul valore dei dati.

L'offerta di servizi gratuiti in cambio di un prelievo massiccio di informazioni consegna ad un numero sempre più esiguo di operatori della rete la possibilità di predire e insieme indirizzare le decisioni di ogni individuo. E su questa base vengono offerti i prodotti di una sofisticata pubblicità mirata sul percorso di navigazione degli utenti, che ripropongono esattamente ciò che era stato oggetto della loro curiosità o desiderio.

In questo modo i giganti di Internet tendono ad occupare, in modo

sempre più esclusivo, ogni spazio di intermediazione tra produttori e consumatori, assumendo un potere che inesorabilmente si traduce anche in un enorme potere politico. Un potere sottratto a qualunque regola democratica.

Il futuro preoccupa ancora di più, con nuovi progetti e nuove applicazioni destinati ad incidere in modo rilevante sulla vita quotidiana, come nel caso dei sensori indossabili o della domotica che traccia, con oggetti intelligenti, ogni nostra azione compiuta anche in casa. Ogni nostro gesto potrebbe finire in un *database*.

Il controllo permea ormai ogni aspetto della nostra esistenza: ad esso siamo purtroppo assuefatti.

Si pensi ai rischi sempre più attuali dei droni per uso civile, dotati di microcamere e in grado di inviare in tempo reale, anche agli *smartphone*, le immagini riprese a distanza ravvicinata. O ancora alla miriade di videocamere diffuse sul territorio, in grado di sfruttare anche tecniche di riconoscimento facciale o segnalare comportamenti anomali.

Su questi fronti il Garante sta già operando sia con autonomi provvedimenti sia concorrendo alla regolamentazione di settore.

Le forme moderne della sorveglianza sono più invasive proprio perché più subdole e difficili da evitare anche quando vengono realizzate sui luoghi di lavoro. Occorre la consapevolezza che anche le attività lavorative sono ormai profondamente condizionate dalle nuove tecnologie, potenzialmente più lesive rispetto alle tradizionali forme di controllo a distanza, e che è dunque necessario ricercare, anche sul piano normativo, nuovi equilibri per salvaguardare la libertà di impresa e il diritto alla riservatezza dei lavoratori.

A tutto questo occorre certo dare risposte giuridiche e tecnologiche, ma soprattutto concepire la protezione dei dati come misura etica della tecnologia e riuscire a gestire i cambiamenti nel rispetto della persona.

I pericoli della Rete tra *hate speech* e cyberbullismo

Maturano in Rete nuove forme di criminalità, dal furto di identità, fino alla più organizzata criminalità cibernetica. È una emorragia stimata in 500 miliardi di dollari l'anno tra identità violate, segreti aziendali razziati, portali messi fuori uso e moneta virtuale sottratta.

Le violazioni troppo spesso coinvolgono sistemi vulnerabili perché non aggiornati e siti programmati senza i migliori standard di sicurezza.

Si pensi alla recente falla *Heartbleed* che ha messo a rischio le informazioni personali di milioni di navigatori (incluse *password*, numeri della carta di credito, *account* bancari), e compromesso i servizi Internet utilizzati quotidianamente, dalla posta elettronica ai *social network*.

Abbiamo motivo di ritenere che nei sistemi di interconnessione telematica, nel nostro Paese, esistano elementi di vulnerabilità sottostimati.

In alcuni casi, poi, la Rete è utilizzata strumentalmente come canale di vessazioni e forme di violenza non di rado rivolte nei confronti dei soggetti più fragili. Tali comportamenti, quando integrino precisi reati, da un lato non possono godere di speciali immunità solo perché realizzati *online*, dall'altro comportano precisi oneri in capo ai *provider* ai quali sia segnalata la presenza di contenuti illeciti: come riconosciuto dalla Corte europea dei diritti dell'uomo e, proprio un mese fa, dalla Corte di giustizia.

Sono sempre più frequenti i casi di incitamento all'odio ma anche fenomeni, quali cyberbullismo e *grooming*, spesso alimentati dalla logica del branco o dall'infondata presunzione di anonimato, e diretti contro un soggetto vulnerabile doppiamente, perché meno consapevole dei pericoli della Rete e maggiormente esposto al trauma che la violenza determina in personalità ancora in evoluzione.

In quanto fenomeno complesso e non riducibile a mera questione

penale, il cyberbullismo non può certo essere affrontato con metodi unicamente repressivi.

L'indirizzo da privilegiare dev'essere quello di un "diritto mite" che pur conservando i presidi di libertà e assenza di censure che connotano la Rete, eviti che essa divenga, da luogo di promozione delle libertà, uno spazio anomico dove impunemente violare la dignità e i diritti.

Il Garante è da tempo attivo in questo campo, soprattutto nella promozione di una reale cultura della "cittadinanza digitale", che responsabilizzi tutti gli utenti della Rete e in particolare i ragazzi.

Ha avuto questo significato la nostra scelta di dedicare, quest'anno, la Giornata europea della protezione dati proprio all'educazione digitale.

Occorre invertire la rotta ed evitare che i giovani siano sfruttati e percepiti soltanto come consumatori passivi di tecnologia, incoraggiandoli a comprendere gli effetti di un uso disinvolto e perfino distorto della Rete e, soprattutto, i rischi che si corrono.

La scuola può e deve svolgere un ruolo di primo piano, prevedendo specifici progetti educativi che insegnino ai giovani a confrontarsi costruttivamente con le nuove forme espressive che la Rete offre loro.

Dal canto loro, educatori e formatori, ma anche genitori e famiglie, devono essere aiutati a colmare il deficit di conoscenza dei nuovi fenomeni e strumenti comunicativi.

Per altro verso occorre favorire l'adozione di dispositivi e configurazioni dei sistemi secondo tecnologie progettate per rispettare la *privacy* e tutelare i minori, mettendo dunque la tecnica al servizio dei diritti.

Su questi temi il confronto avviato, in particolare, con il Parlamento e gli altri soggetti istituzionali coinvolti potrà offrire indicazioni importanti per contrastare fenomeni che chiamano in causa la responsabilità e l'impegno di tutti.

L'Autorità fra tradizione e governo dell'innovazione

Nonostante le difficoltà, comincia ad affermarsi il principio che non esistono zone franche - nemmeno su Internet - in cui sia possibile violare impunemente le regole.

In seguito all'accertamento di pregresse violazioni, abbiamo disposto nei confronti di *Google* una sanzione di un milione di euro. La società si è prontamente adeguata alle misure prescritte.

Nei confronti della stessa è in corso un nuovo procedimento, in coordinamento con le altre Autorità europee, riguardante il complesso delle attività di profilazione degli utenti.

In questo quadro, la recente sentenza della Corte di giustizia su *Google Spain* non solo ha spostato l'equilibrio tra potere della tecnologia e quello del diritto a favore del secondo ma ha, per la prima volta, riconosciuto la competenza territoriale di un Paese europeo e il conseguente necessario obbligo al rispetto della direttiva sulla protezione dei dati.

In tale contesto, va segnalato che *Google* e *Facebook* hanno recentemente manifestato la volontà di una nuova e profonda revisione delle loro regole per la *privacy*.

La decisione assunta da *Google* sul diritto all'oblio va salutata favorevolmente, anche se andranno verificate concretamente le modalità di bilanciamento dei diritti del singolo con la memoria collettiva.

Il ruolo delle Autorità resta in ogni caso ineludibile.

Si è aperta una fase nuova e affascinante che spinge tutti gli attori ad affrontare con più responsabilità le contraddizioni della Rete, a ricercare nuovi equilibri tra fattibilità tecnica, accettabilità giuridica e fondamento etico della società digitale.

Ulteriori rischi per gli utenti derivano dalla proliferazione delle applicazioni che quotidianamente scarichiamo sui nostri dispositivi

in un contesto di frammentazione dei soggetti coinvolti nello sviluppo e nella distribuzione, raccolta massiccia dei dati, mancanza di trasparenza e scarse misure di sicurezza.

In questa prospettiva l'Autorità ha avviato una verifica delle applicazioni mediche (ad oggi circa 17mila) disponibili sui nostri dispositivi che offrono terapie personalizzate, monitoraggio della salute, servizi di diagnosi e cura, ma che trattano dati sensibili, quanto di più delicato appartenga ad una persona.

Per altro verso, nell'ambito delle attività economiche, ci siamo impegnati per favorire il rispetto delle regole attraverso uno sforzo costante di semplificazione, con l'obiettivo di coniugare al più alto livello i diritti dei cittadini con le esigenze delle imprese.

Con questo spirito l'Autorità, con crescente frequenza, ha coinvolto le categorie interessate attraverso consultazioni pubbliche e tavoli di lavoro, con il proposito di promuovere un ampio confronto sulle soluzioni da adottare alleggerendo, ove necessario, oneri sproporzionati o non realmente efficaci.

Con un importante provvedimento sui *cookie*, condiviso con gli operatori, abbiamo indicato un nuovo modello di espressione del consenso degli utenti sull'uso dei loro dati di navigazione.

Abbiamo introdotto una disciplina organica e innovativa dei sistemi biometrici, contente rilevanti semplificazioni degli adempimenti e, recentemente, adottato un primo provvedimento sui servizi di *mobile payment*: servizi apprezzabili che, però, prevedono una concentrazione imponente di informazioni in capo a operatori telefonici, banche e altri soggetti.

Nell'ottica di garantire che le logiche di mercato non configurino inaccettabili invasioni della sfera privata e domestica delle persone, siamo ancora intervenuti sul *telemarketing* - con accertamenti ispettivi

e sanzioni pesanti emesse nei confronti di società specializzate - e sul fenomeno delle telefonate "mute", con un provvedimento specifico che ha eliminato gli effetti distorsivi di questa pratica commerciale, senza tuttavia penalizzare l'efficienza delle imprese.

Con lo scopo di affrontare le insidie dello *spam* - come quelle diffuse sui *social network* - abbiamo adottato delle Linee guida che contengono un quadro unitario di misure utili non solo a chi vuole difendersi da tali invadenze, ma anche alle imprese per programmare campagne pubblicitarie conformi alle norme.

Per favorire una maggiore consapevolezza dei diversi soggetti coinvolti, abbiamo intensificato l'attività di comunicazione attraverso apposite guide in tema di *privacy* nei *social network*, scuola, condominio, *cloud computing*, imprese.

Il diritto alla *privacy* non si confronta solo con la tecnologia delle comunicazioni ma anche con la scienza applicata al corpo e alla vita, la biotecnologia, tanto preziosa quanto bisognosa di un quadro giuridico di riferimento.

In questo senso la protezione dati gioca un ruolo centrale nel rapporto tra tecnica e natura, il corpo e i suoi limiti. Si pensi a temi nuovi ed estremamente delicati quali quelli della fecondazione assistita (come ha dimostrato il recente caso dell'ospedale Pertini), dell'anonimato materno e, più in generale, della non coincidenza tra genitorialità elettiva e biologica.

Quando il Parlamento, in ossequio alle recenti sentenze della Consulta, dovrà legiferare, il Garante sarà ovviamente pronto a fornire il proprio contributo, al fine di coniugare al meglio il diritto del nato a conoscere le proprie origini con il diritto all'anonimato del genitore naturale.

La protezione dei dati come fattore di sviluppo del Paese

L'Autorità è particolarmente impegnata per garantire che l'adeguamento di ogni settore della pubblica amministrazione si realizzi in un quadro di tutela dei cittadini.

Efficienza, trasparenza, produttività, sono gli obiettivi che tendono a giustificare e legittimare le spinte verso un'amministrazione sempre più aperta.

Quanto più cresce la raccolta di dati, per ragioni di controllo della spesa pubblica o di giustizia, tanto più cresce il diritto dei cittadini a pretendere un uso lecito di tali dati, nel rispetto degli altri diritti costituzionalmente garantiti.

L'Autorità ha svolto un'intensa attività affinché lo scambio di dati e la loro accessibilità siano sempre realizzati in una cornice di regole il cui rispetto è la condizione essenziale per garantire la certezza che le informazioni vengano utilizzate unicamente per finalità legittime e, soprattutto, protette da accessi illeciti.

Positiva è stata la nostra collaborazione sulla disciplina di alcune banche dati strategiche, come il sistema di prevenzione delle frodi e dei furti d'identità, e sul regolamento di attuazione dell'anagrafe nazionale della popolazione residente destinata a contenere tutti i dati anagrafici dei cittadini e accessibile a tutte le amministrazioni, punto di partenza strategico per la realizzazione di una pubblica amministrazione digitale.

Consideriamo una priorità garantire la sicurezza e l'integrità delle banche dati che, per le specifiche finalità per cui sono state costituite, per la qualità dei dati in esse raccolti e per la quantità dei soggetti censiti, sono da considerarsi sempre di più luoghi di possibili abusi.

Abbiamo svolto un lavoro impegnativo per indicare regole e misure, di natura tecnica e organizzativa, necessarie per tutelare

le informazioni raccolte e archiviate, come nel caso dei provvedimenti adottati nei confronti di Sogei o al parere espresso per consentire l'accesso diretto alle banche dati INPS da parte delle pubbliche amministrazioni per finalità istituzionali.

Di particolare rilievo è stata la verifica preliminare sul cosiddetto "redditometro".

In collaborazione con l'Agenzia delle entrate, abbiamo individuato il giusto equilibrio tra legittime esigenze di contrasto all'evasione fiscale e il diritto dei cittadini affinché siano utilizzate soltanto informazioni pertinenti, impedendo illegittime profilazioni dei contribuenti basate sull'individuazione presuntiva delle spese.

Non esiste alcun conflitto tra l'interesse di quanti gestiscono una banca dati e il diritto delle persone cui i dati appartengono.

Un'infrastruttura vulnerabile agli attacchi informatici è un'infrastruttura inefficiente, rischiosa per la propria funzione, per l'azione amministrativa, per la qualità dei servizi offerti, in alcuni casi per la stessa sicurezza dello Stato, oltre che per quella dei singoli cittadini.

Spetta dunque alle Istituzioni dimostrare, prima di chiunque altro, che un equilibrio tra efficienza, innovazione e rispetto dei diritti è possibile.

Tanto più in considerazione degli enormi cambiamenti strutturali che il Paese dovrà affrontare per dare piena attuazione all'Agenda digitale.

Privacy e trasparenza

La trasparenza è un'istanza sempre più forte, in quanto funzionale al controllo democratico sull'esercizio del potere pubblico e sull'azione amministrativa. La pubblicazione degli atti amministrativi in rete è, in questo senso, uno strumento insostituibile per comprendere come il potere pubblico viene amministrato, come agiscono le Istituzioni,

come vengono gestite le procedure selettive e concorsuali, come sono spesi e che destinazione hanno i soldi pubblici.

Tuttavia sono necessarie alcune essenziali cautele, volte a proteggere la dignità delle persone e non certo a garantire opacità ai processi decisionali o ad interessi di parte.

In questa direzione si è mosso il Garante nell'interpretazione del nuovo ordinamento in materia di trasparenza, resa con apposite Linee guida contenenti indicazioni per la migliore attuazione delle norme che comportino la pubblicità di dati di persone fisiche.

Le Linee guida suggeriscono, in particolare, accorgimenti utili a garantire tanto la trasparenza quanto la tutela dei dati personali. L'obiettivo è quello di impedire l'alterazione o la decontestualizzazione, suscettibili di pregiudicare non solo i diritti individuali, ma anche la stessa qualità delle informazioni.

Con le stesse abbiamo indicato alcune indispensabili cautele per i dati sensibili, la cui indebita pubblicità in Rete potrebbe esporre a gravi discriminazioni.

La *privacy* non contrasta, ma anzi può contribuire a valorizzare la trasparenza dell'azione amministrativa, mediante un'adeguata selezione delle notizie davvero funzionali all'esercizio del controllo diffuso di legalità.

Abbiamo bisogno di trasparenza, ma solo di una buona trasparenza, che non comprima sbrigativamente i diritti fondamentali nel segno di una facile demagogia.

In questo spirito, con un provvedimento specifico, il Garante ha fissato un quadro organico di regole per l'uso trasparente dei dati dei cittadini in un ambito delicato come quello dei partiti politici e ha fornito indicazioni al Parlamento sulla pubblicità delle contribuzioni agli stessi erogate dai cittadini.

La riservatezza: tra democrazia dell'informazione e mediatizzazione della vita privata

La centralità assunta dalla Rete nel sistema mediatico e la stessa tendenza a diffondere notizie mediante *blog* e *social network* hanno profondamente mutato il modo di fare informazione. La sola circostanza della pubblicazione in Rete cambia infatti, e molto, l'informazione e il suo impatto sulle persone, consentendo di rintracciare, anche a distanza di anni, dati che a volte restituiscono una rappresentazione solo parziale, perché non aggiornata, di vicende individuali, riducendo la complessità di una vita a un istante o un dettaglio, magari fuorvianti o comunque poco rappresentativi.

Tali temi sono stati oggetto di particolare attenzione nel corso dei lavori preliminari all'adozione di un aggiornamento del Codice deontologico dei giornalisti, risalente a 15 anni fa, che si sono svolti in un lungo e articolato confronto con la presidenza dell'Ordine.

La bozza elaborata codificava, in particolare, alcune misure volte a coniugare diritto all'oblio e libertà di stampa, tentava di declinare il principio di lealtà e correttezza dell'informazione con riguardo alla raccolta delle notizie attraverso dispositivi occulti o con raggiro, introduceva specifiche garanzie per le minoranze e i soggetti meno tutelati (dai minori ai malati, dagli arrestati ai rifugiati).

La bozza introduceva anche, secondo i principi del Consiglio d'Europa, una specifica e organica disciplina della cronaca giudiziaria, con una particolare attenzione ai terzi a vario titolo coinvolti nel procedimento penale, rispetto a fatti privi di interesse pubblico e attinenti alla sfera più intima degli stessi.

Tale, in particolare, era l'indirizzo che ispirava l'ipotesi di disciplina della divulgazione dei dati inerenti la vita privata delle persone (soprattutto se non indagate) acquisiti con strumenti

investigativi tanto preziosi quanto invasivi, come le intercettazioni.

Con riferimento a queste si proponeva, in particolare, di dare notizia di tutto ciò che avesse rilievo pubblico, ma nel rispetto della dignità di ciascuno, ed espungendo dettagli di vita privata, spesso intimi, privi di rilievo ai fini di una corretta informazione dei cittadini. Privilegiando i contenuti rispetto alla trascrizione letterale.

Nonostante una sostanziale e non residuale convergenza emersa durante i lavori, il Consiglio nazionale dell'Ordine ha deciso di non approvare i contenuti proposti.

Pensiamo che si sia persa un'occasione importante per affrontare i numerosi problemi aperti e tuttora irrisolti, attraverso gli strumenti dell'autodisciplina e al di fuori di interventi autoritativi del legislatore.

*****

Anche nel corso di quest'anno l'impegno del Collegio è stato costante e intenso.

Nel 2013 abbiamo adottato 606 provvedimenti collegiali, inclusi 222 ricorsi e 22 pareri resi al Governo e al Parlamento. Quasi 32.000 sono i quesiti ai quali l'Ufficio ha dato risposta, 850 sono state le sanzioni contestate, più di 411 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, destinata ad aumentare, con importante riconoscimento per il lavoro svolto, anche in ambito internazionale, dove proficui sono i rapporti con le altre Autorità.

Possiamo contare sull'apporto prezioso di un Ufficio dotato di personale giovane e altamente specializzato che lavora con passione e dedizione, nonostante l'esiguità dell'organico.

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI