GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Persona vulnerabile

La protezione dei dati nella società digitale

Discorso del Presidente

Antonello Soro

Relazione2014

Relazione2014

Discorso del Presidente

Antonello Soro

Roma, 23 giugno 2015

Signor Presidente della Repubblica,

Signora Presidente della Camera,

Autorità, Signore e Signori,

L'importanza strategica della protezione dei dati

Il progresso e l'innovazione hanno profondamente modificato i nostri modi di vivere, di abitare il mondo, di organizzarlo.

Non solo per le trasformazioni evidenti nei sistemi di comunicazione ma per quelle ancora più rilevanti nelle relazioni economiche, con lo sviluppo dell'economia digitale fondata sui dati, che ridisegna una geografia globale del potere.

Sono cresciute imprese capaci di sconvolgere i meccanismi consolidati della concorrenza, di concentrare nella loro disponibilità tutto il sapere che sette miliardi di persone, individualmente, generano ogni giorno.

È lo sviluppo esponenziale dei Big data, alimentato dall'uso intensivo di tecniche di calcolo sempre più raffinate e precise.

È l'Internet delle cose, con le sue molteplici applicazioni, dalla domotica alle tecnologie indossabili, che attribuisce anche agli oggetti di uso comune un'identità digitale.

È il "pianeta connesso", nuova dimensione delle nostre esistenze che raccoglie non solo le tracce lasciate dal web, ma anche dai geolocalizzatori, dai droni, dai dispositivi intelligenti che elaborano, in tempo reale, perfino dati emotivi e dinamici.

In questa rete pervasiva di oggetti, che interagiscono e comunicano costantemente, l'uomo rischia davvero di ridursi ad un supporto: da analizzare e osservare nei comportamenti, da profilare per condizionarne le scelte,

da sorvegliare per realizzare un controllo sempre più invasivo che di fatto si estende alle nostre abitazioni, alla nostra fisicità.

Tutto ruota intorno ad una raccolta onnivora di dati.

Ma nella società digitale noi siamo i nostri dati e la vulnerabilità dei dati è vulnerabilità delle nostre persone: da questa considerazione si deve partire per ricercare nuove e più efficaci forme di tutela delle nostre libertà.

Ad essere analizzate, sezionate ed elaborate sono oggi le nostre identità affidate ad algoritmi che orientano non solo settori rilevanti dell'economia, della politica, della finanza, ma sempre di più le nostre scelte quotidiane.

Dalla telemedicina alle consultazioni politiche on-line; dalla giustizia telematica al fascicolo sanitario elettronico; dalla videosorveglianza ai social network alle applicazioni per il *live streaming* come *Periscope*; dalla stampa on-line all'analisi genetica del crimine.

Non c'è dimensione della vita, privata e pubblica, che non presupponga un trattamento di dati personali e non richieda solide garanzie per evitare che quei dati vengano usati "contro di noi", privandoci della nostra libertà anziché agevolandone l'esercizio.

Questo mutamento profondo nell'organizzazione della vita quotidiana stimola interrogativi e inquietudini, mette in luce le contraddizioni legate alla pluralità di dimensioni in cui la vita reale si svolge, ripropone il tema delicato del rapporto tra uomo e macchina, il timore represso che l'intelligenza artificiale possa autonomizzarsi dall'uomo e insieme la tentazione di delegare alle tecnologie scelte e decisioni che all'uomo competono.

Gli scenari della società digitale disegnano un quadro di grandi sfide che abbiamo il dovere di affrontare senza rassegnata subalternità e senza inutile ostilità.

Dobbiamo rimuovere la tentazione tecnofobica, il timore dell'innovazione, senza rinunciare a contrastarne le distorsioni, a ricercare una qualche regolazione dei processi e, più in generale, a vivere responsabilmente il nostro tempo.

In questo quadro la protezione dei dati si pone non solo come diritto confinato alla sfera dell'intimità, ma come insostituibile chiave per mantenere l'equilibrio tra fattibilità tecnica ed accettabilità giuridica, tra etica e progresso, presupposto per l'esercizio delle altre libertà.

È utile registrare come non solo la Cassazione ma anche l'ONU, con singolare sincronia, abbiano recentemente sancito il principio che i diritti devono godere on-line della stessa tutela accordata off-line e che l'identità digitale non è meno "personale" di quella reale.

In questa cornice di cambiamenti si dispiega l'attività del Garante.

Per un'informatizzazione della Pubblica Amministrazione attenta al valore dei dati personali

La vulnerabilità di dati non protetti ha effetti dirompenti sulla loro integrità, correttezza e disponibilità.

Non c'è protezione dei dati senza sicurezza e garantire la sicurezza è sempre più difficile, considerato l'aumento esponenziale della criminalità informatica, di cui tutti siamo potenziali vittime: dai furti di identità, di *account* personali, alla violazione dei sistemi di pagamento elettronico fino ai blocchi di computer con finalità estorsiva.

La prima sfida per l'Autorità è quella di promuovere, nel pubblico e nel privato, un approccio sistematico alla protezione dei dati e delle infrastrutture.

Nella pubblica amministrazione digitale, la sicurezza è un obiettivo chiave per costruire la fiducia dei cittadini e per garantire efficienza e trasparenza.

L'attività del Garante si è articolata nella verifica e prescrizione di misure di sicurezza, relative ai sistemi di archiviazione, ai flussi dei dati, alla interoperabilità delle banche dati condivise tra le amministrazioni dello Stato, gli enti locali, gli organismi di previdenza, le varie agenzie.

I numerosi provvedimenti adottati, spesso all'esito di accertamenti ispettivi, sono stati il frutto di una proficua attività di collaborazione con le

amministrazioni che hanno abitualmente recepito le nostre indicazioni.

Un notevole impegno abbiamo profuso per aumentare il livello di sicurezza dello SPID - sistema pubblico utilizzato per gestire le identità digitali - destinato a diventare vera e propria infrastruttura critica, dalla cui efficienza e affidabilità dipenderà la possibilità di fruire di servizi on-line con piena fiducia da parte dei cittadini.

Anche la realizzazione di un moderno ed efficiente sistema fiscale passa per la creazione di nuove banche dati e per l'implementazione e l'interconnessione di quelle esistenti.

Numerosi sono i pareri resi all'amministrazione finanziaria e, tra quelli più recenti, i correttivi richiesti ed introdotti dall'Agenzia delle entrate sul modello 730 precompilato che hanno consentito di individuare modalità tecniche per garantire accessi sicuri, tracciabili e selezionati ai dati dei contribuenti.

Ugualmente nel settore sanitario: la conservazione digitale della cartella clinica, la refertazione on-line, il fascicolo sanitario ed il dossier sanitario sono alcuni dei nostri principali interventi.

E dove è stata accertata, nell'ambito delle numerose istruttorie svolte, l'inadeguatezza dei sistemi, sono stati adottati specifici provvedimenti di blocco, come nel caso di alcune importanti aziende ospedaliere.

L'innovazione tecnologica deve necessariamente essere accompagnata da sistemi di sicurezza informatica che garantiscano autenticazione dei dati, la loro tracciabilità, accessi selettivi con credenziali univoche, cifratura, sistemi di alert e attività di auditing: queste sono alcune delle principali aree di intervento dell'Autorità nell'effettuare le valutazioni con riferimento a tutti gli ambiziosi progetti di modernizzazione dell'Italia.

E per combattere le nuove vulnerabilità della società digitale.

Che si aggiungono alle vecchie e non meno delicate: penso ad esempio al malato di HIV che deve chiedere l'esenzione allo sportello della Asl in cui lavora, o allo studente che ha cambiato sesso e deve esibire il certificato di laurea o al caso controverso dell'anonimato materno.

Per una protezione dei dati davvero dinamica e funzionale

Avvertiamo la responsabilità di rendere effettivi i princìpi del nostro Codice superando, ove possibile, informative dispersive, prescrivendo soluzioni compatibili con la realtà.

Abbiamo consolidato percorsi virtuosi di confronto con gli operatori per definire regole condivise e tecnicamente implementabili.

Rispetto alle rigide soluzioni che rendono di fatto le norme inattuabili abbiamo ricercato forme nuove, come per i *cookie* e il *mobile payment* che, senza ostacolare le esperienze degli utenti, ne richiedono una consapevole interazione.

La semplificazione deve però essere sempre accompagnata da serie politiche di trasparenza.

È nostro impegno costante impedire lo sfruttamento dei dati dei consumatori senza peraltro sottovalutare le esigenze del mercato, come nel parere reso al Ministero dell'economia sul sistema di prevenzione dei furti di identità nel settore del credito al consumo.

Nei rapporti di lavoro il crescente ricorso alle tecnologie nell'organizzazione aziendale, i diffusi sistemi di geolocalizzazione e telecamere intelligenti hanno sfumato la linea – un tempo netta – tra vita privata e lavorativa.

È auspicabile che il decreto legislativo all'esame delle Camere sappia ordinare i cambiamenti resi possibili dalle innovazioni in una cornice di garanzie che impediscano forme ingiustificate e invasive di controllo, nel rispetto della delega e dei vincoli della legislazione europea.

Un più profondo monitoraggio di impianti e strumenti non deve tradursi in una indebita profilazione delle persone che lavorano.

Occorre sempre di più coniugare l'esigenza di efficienza delle imprese con la tutela dei diritti: obiettivo che ha ispirato tutte le decisioni dell'Autorità nelle numerose verifiche preliminari nonché nelle linee guida in materia di biometria.

Nel settore privato, abbiamo avviato puntuali accertamenti per verificare

il rispetto delle prescrizioni, a suo tempo impartite alle banche, al fine di innalzare i livelli di sicurezza dei sistemi e dei dati dei correntisti.

La sicurezza del resto ha un ruolo centrale nel nuovo Regolamento UE – giunto alla fase finale – che spinge, tra l'altro, verso l'adozione di modelli che incorporano la sicurezza dei dati direttamente nelle tecnologie, promuove valutazioni di impatto ed analisi dei rischi ed assegna alle Autorità nuovi e rilevanti compiti come nel caso dei sistemi di certificazioni europee.

La protezione dei dati bussola nel futuro digitale

L'economia digitale ha favorito una concentrazione di potere in mano a piattaforme tecnologiche sempre più esclusive e protagoniste influenti delle relazioni internazionali.

E tuttavia, a partire dalle sentenze della Corte di giustizia, si è aperta una fase nuova.

Il Parlamento europeo, nel novembre 2014, ha approvato una Risoluzione che punta a separare l'attività dei motori di ricerca dagli altri servizi e la Commissione ha aperto una procedura di infrazione per presunto abuso di posizione dominante di Google.

Sono segnali importanti, un freno reale al dilagare senza condizioni del potere delle piattaforme, anche se l'Europa non può ignorare la propria responsabilità per il grave ritardo nella costruzione di un mercato digitale davvero competitivo, prima causa della sua dipendenza tecnologica.

Da tempo la nostra Autorità lavora con l'obiettivo di rimuovere l'asimmetria informativa e l'opacità dei soggetti che dominano il mercato digitale.

Il nostro provvedimento prescrittivo nei confronti di Google punta ad imporre al gigante di internet le stesse regole cui sono tenute le imprese europee.

E il protocollo di intesa sottoscritto, il primo in Europa, assoggetta l'azienda a verifiche periodiche presso la sede californiana (la prima si è svolta a maggio) per monitorare il rispetto delle nostre prescrizioni ma, insieme, permette

un confronto costruttivo e dialogante su temi normalmente oggetto di riserbo assoluto da parte della società americana.

La procedura per un corretto esercizio del diritto all'oblio è stata incardinata e costringe i motori di ricerca a porsi come nostri interlocutori spingendoli a confrontarsi con problematiche complesse che non trovano soluzione soltanto nella tecnologia.

In questo primo anno le richieste di oblio sono state respinte nel 73% dei casi, secondo criteri e valutazioni che il Garante, adito successivamente al rigetto, ha generalmente condiviso.

Abbiamo tracciato un sentiero, dimostrando come la protezione dei dati possa davvero essere la chiave attraverso la quale presidiare le complessità dello spazio digitale.

In questo senso vorrei ricordare il parere sul Programma statistico nazionale, che prevede la possibilità di utilizzare per la prima volta anche i Big data o la consultazione attualmente aperta sull'Internet delle cose o gli accertamenti avviati – a livello internazionale – con riguardo al complesso mondo delle applicazioni, in particolare quelle che offrono servizi ai minori o consentono di monitorare la nostra salute.

Siamo immersi nella società digitale e sempre di più conosciamo noi stessi, il mondo e gli altri attraverso la tecnologia, senza disporre dei necessari anticorpi.

Per questo c'è bisogno di una nuova "alfabetizzazione" che promuova comportamenti attivi e informati per gestire con prudenza i nostri dati e, dunque, anche l'approccio divulgativo diventa parte essenziale dei compiti dell'Autorità.

Tutte le Istituzioni sono chiamate ad un supplemento di impegno per ridurre e cancellare la distanza che separa la tutela dei cittadini nello spazio digitale rispetto a quelle consolidate e garantite nello spazio fisico.

Come è stato per la cultura ambientalista, occorre infatti diffondere la consapevolezza che anche nell'Infosfera ogni atto compiuto deve essere un atto responsabile e che il contributo di ciascuno, oggi, è indispensabile per

migliorare la prospettiva del nostro futuro e tracciare uno sviluppo sostenibile del pianeta connesso. E questa è sfida che interroga gli Stati ed esige una risposta globale.

Una Kyoto della protezione dati.

Privacy e sicurezza: sinergia, non antitesi

La dimensione digitale sarà sempre più il teatro dei conflitti internazionali.

Il Datagate ha mostrato sia l'insostenibilità democratica sia la sostanziale inefficacia della legislazione emergenziale fondata sulla raccolta generalizzata e indiscriminata delle comunicazioni, con un'inaccettabile quanto inutile compressione del diritto alla privacy.

Quell'esperienza ha indotto gli Usa a orientarsi verso il modello europeo di bilanciamento tra libertà e sicurezza, ben espresso dalla Corte costituzionale tedesca: "la Costituzione esclude il perseguimento della sicurezza assoluta al prezzo della libertà".

Eppure, mentre negli Usa cresce l'adesione a questo modello l'Europa, nella percezione della propria fragilità, rischia di rinnegare se stessa. Come smarrita davanti alla crescente asimmetria che il diritto presenta rispetto a una tecnologia in continua evoluzione e, insieme, alle pulsioni securitarie dell'opinione pubblica.

Ne abbiamo colto un segnale nelle leggi approvate in questi mesi in Spagna e Francia.

E nel percorso del nostro decreto anti-terrorismo.

In fase di conversione, a quel provvedimento – sul cui testo originario siamo stati auditi dalla Camera, oltre che dal Csm – sono state aggiunte una serie di previsioni che – l'abbiamo segnalato – avrebbero alterato il giusto equilibrio tra privacy e sicurezza, sottovalutando anche le implicazioni di alcune tecnologie.

Come nel caso delle intercettazioni da remoto, con il rischio di un serio ostacolo al controllo di legittimità sui dati acquisiti.

È stato un atto di saggezza sia lo stralcio di questa norma sia le opportune

modifiche apportate alle previsioni che, da un lato, ammettevano le intercettazioni preventive per qualsiasi reato commesso on-line e che, dall'altro, estendevano "a regime", in misura rilevante e non selettiva il tempo di conservazione dei dati di traffico.

Questo, in palese contrasto con le indicazioni fornite dalla Corte di giustizia 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 il personale che nell'Ufficio, ogni giorno, lavora con generosità e competenza per dare risposta alle crescenti domande di tutela dei cittadini.