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, 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.

Occorre sempre di più coniugare l'esigenza di efficienza delle imprese con la tutela dei diritti: obiettivo che ha ispirato 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.

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