GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

La protezione dei dati diritto di libertà

Discorso del Presidente

Antonello Soro

Relazione2015

Relazione2015

Discorso del Presidente

Antonello Soro

Roma, 28 giugno 2016

Signor Presidente del Senato,

Autorità,

Signore e Signori,

Desidero innanzitutto ringraziare il Presidente del Senato per l'ospitalità e per le sue parole.

Vorrei inoltre esprimere un particolarissimo ringraziamento al Presidente della Repubblica, al quale ieri abbiamo presentato la Relazione, e che non ha mai mancato di offrirci attenzione e sostegno.

Proprio mentre l'Europa vive una crisi senza precedenti si è concluso il lungo percorso di approvazione del nuovo Regolamento sulla protezione dati e della Direttiva sulle garanzie applicabili nelle attività di polizia e giustizia.

Riforme alle quali l'Autorità ha collaborato attivamente, dedicando una parte rilevante delle proprie energie.

Il nuovo quadro giuridico porta grandi novità rafforzando la tutela dei diritti, nel segno della responsabilità delle imprese e della semplificazione delle procedure.

Nel momento in cui si fanno più forti le spinte anacronistiche a creare "barriere" alla libera circolazione di beni e persone, il Regolamento raggiunge l'ambizioso obiettivo di assicurare una disciplina armonizzata tra gli Stati membri, eliminando definitivamente le numerose asimmetrie create nel tempo.

Ma, soprattutto, la sua approvazione permette di affrontare una delle sfide più importanti che il legame tra tecnologia, nuovi diritti e strategie di prevenzione pone alle nostre democrazie: la convergenza globale nella tutela

di un diritto - quello alla protezione dati - che rappresenta il primo presupposto di libertà nella società digitale.

L'Europa ha oggi la straordinaria opportunità di proporre, su scala mondiale, il proprio modello di protezione dei dati quale autentica bussola nel pianeta connesso, capace di coniugare al punto più alto i diritti delle persone con le esigenze del mercato.

E può diventare - nella chiave di una maggiore protezione dei cittadini - lo strumento attraverso il quale le nostre imprese possono competere con i giganti del web e trovare un ruolo non subalterno nella geografia dell'economia mondiale.

Le nuove frontiere tecnologiche: promuovere un uso etico dei dati

Lo sviluppo e la diffusione delle tecnologie hanno cambiato in profondità l'organizzazione delle nostre vite.

Dalle forme più evolute di comunicazione in rete siamo passati al consumo collaborativo della sharing economy, all'Internet delle cose, ad ambienti connessi dove anche gli oggetti dialogano autonomamente tra loro.

Il tema della protezione dei dati si intreccia con le nuove realtà che, come la domotica o le tecnologie indossabili, hanno amplificato a dismisura la capacità di raccogliere, archiviare e sfruttare informazioni.

L'intelligenza artificiale attraverso lo sviluppo dell'apprendimento automatico mette sempre più in tensione il rapporto tra uomo e macchina e si spinge verso frontiere inesplorate, rendendo possibili sperimentazioni in grado di connettere le persone anche nella loro fisicità.

Connettere il corpo umano - a partire dai dispositivi medici impiantabili, a sistemi per la stimolazione cerebrale fino ai chip di facilitazione nella vita quotidiana - comporta nuove pericolose vulnerabilità, con inaspettati scenari di hackeraggio e di controllo pervasivo che potrebbero estendersi ai nostri pensieri ed emozioni.

Per altro verso avanza la ricerca in campo genetico, sviluppando attitudini predittive e manipolative che ci espongono ad inedite e imprevedibili minacce.

Da un lato gli enormi potenziali dei Big data consentono di ricavare, come in un mosaico, informazioni personali anche da frammenti di dati apparentemente privi di elementi identificativi; dall'altro il crescente mercato del Cloud computing e delle sue evoluzioni, la frammentazione dei soggetti e dei processi che elaborano i dati, anche per tempi illimitati, amplificano i rischi di una definitiva perdita di controllo su di essi e di una sorveglianza capillare sulla nostra esistenza.

Fenomeni la cui dimensione globale ha spinto le Autorità di garanzia a fare rete ed organizzarsi avviando, tramite il GPEN (Global Privacy Enforcement Network), attività di cooperazione anche attraverso indagini mirate sul piano internazionale.

Pensiamo che per contenere un uso distorto ed "incontrollato" dei nostri dati sia indispensabile promuovere una maggiore consapevolezza sulle intrinseche ambivalenti potenzialità che ogni tecnologia può comportare.

La chiave per garantire la sostenibilità dei profondi mutamenti in atto sta nella capacità di coglierne le opportunità, rafforzando i valori che ci appartengono, non facendosi abbagliare dal fascino di tutto quello che tecnicamente è possibile.

Per questo dobbiamo contrastare l'idea che sia inesorabile una progressiva riduzione degli spazi di libertà ed intimità individuale che hanno rappresentato il fondamento delle democrazie liberali del ventesimo secolo.

Per questo è realistico sostenere che nel nostro tempo la protezione dei dati sta alla società digitale come le garanzie dei lavoratori e le preoccupazioni per l'ambiente sono state rispetto allo sviluppo industriale del secolo scorso.

Questioni complesse che impongono adeguate scelte sociali e, soprattutto, politiche per assicurare in ogni contesto un utilizzo davvero responsabile ed eticamente accettabile dei nostri dati.

Una economia fondata sui dati

I nuovi modelli di sviluppo favoriscono l'accumulo di ricchezza in ragione dell'agevole accessibilità e disponibilità dei dati degli utenti, oggetto di una crescente mercificazione.

La concentrazione del potere di profilazione in capo a poche aziende, presupposto per un oligopolio della intermediazione tra produttori e consumatori, condiziona sempre più il mercato mondiale dei consumi e, più in generale, orienta le scelte personali.

Dalle tradizionali forme di monitoraggio in rete dei nostri comportamenti siamo passati ad ancor più sofisticati sistemi di analisi dei social network o all'uso di app intelligenti che anticipano, in modo proattivo, le nostre richieste.

Si pone un generale problema di libertà, se nell'economia fondata sui dati non siamo capaci di proteggere i dati.

La dimensione digitale della vita, nel suo dispiegarsi senza confini di spazio e di tempo, non è necessariamente anomica e le Autorità garanti, confortate dalla giurisprudenza europea, hanno iniziato ad esercitare la propria funzione anche rispetto alle multinazionali della rete.

In questa cornice, consolidata la procedura di confronto e controllo, appena conclusa, con Google - che peraltro ha dato piena attuazione alle prescrizioni finora impartite - siamo di recente intervenuti sul delicato tema dell'accesso ai dati pubblicati con falso account, riaffermando la nostra competenza anche nei confronti di Facebook.

Un diritto sempre più universale

Nel 2015 l'emergenza terrorismo si è posta al centro dell'agenda politica, proprio nel momento in cui la privacy iniziava ad essere percepita - oltre che formalmente sancita - quale presupposto intangibile di libertà e dignità della persona.

Le esperienze di questi anni hanno dimostrato come l'attività d'intelligence, che può avvalersi di tecnologie tanto efficaci quanto pervasive e suscettibili di

abusi, necessiti di regolamentazione e di cautele rigorose, per impedire che funzioni volte a garantire la democrazia, finiscano per violarla.

Non a caso il tema delle garanzie rispetto all'attività di prevenzione è stato oggetto di importanti sentenze delle supreme giurisdizioni interne e sovranazionali.

A partire dalla sentenza costituzionale portoghese di agosto fino a quelle della Corte europea dei diritti dell'uomo, l'orientamento comune indica la necessità di un vaglio intrinseco, da parte di organi terzi, sulle misure d'intelligence, quali in particolare le intercettazioni preventive, a tutela dei diritti dei cittadini.

Tutela cui contribuisce anche la nostra attività per consolidare le garanzie rispetto al potere investigativo.

In questo quadro è ineludibile l'esigenza, avvertita anche dalla giurisdizione, di delimitare i presupposti per applicare, a strumenti d'indagine tradizionali, tecnologie capaci di mutarne profondamente natura e incidenza sui diritti fondamentali.

Come nel caso dei software-spia utilizzati per le intercettazioni ambientali, che trasformano un mezzo investigativo comunque "circoscrivibile" in uno strumento di sorveglianza totale perché "ubiquitario", potenzialmente applicabile senza limiti di spazio né di tempo.

È, infatti, quella della tecnologia la dimensione in cui oggi, più di ogni altra, il rapporto tra libertà e sicurezza, privacy e prevenzione, assume forme nuove e costringe a ripensare categorie giuridiche consolidate: dall'uso dei social network per fini di propaganda terroristica alla genetica forense con le varie banche dati del DNA, al data mining.

Ed è proprio la garanzia della riservatezza di fronte alle potenzialità della tecnologia una delle componenti essenziali della legge statunitense di febbraio, volta ad assicurare una tutela remediale ai cittadini stranieri i cui dati personali siano acquisiti da agenzie americane.

Un atto che, insieme al nuovo tentativo di accordo con la Commissione Ue sul Privacy Shield, si è reso necessario per stabilire rapporti più equilibrati - anche commerciali - tra Europa e Stati Uniti.

Rapporti seriamente compromessi dalla vicenda del Datagate a seguito della quale la Corte di giustizia ha appunto dichiarato invalido il Safe Harbour, strumento che per lungo tempo aveva regolato il trasferimento dei dati tra le due sponde dell'Atlantico.

Le persistenti difficoltà nel negoziato sul Privacy Shield sono per noi motivo di forte preoccupazione.

Le Autorità garanti sono destinatarie di un obbligo di contrasto e di sanzione nei confronti delle imprese che continuano a trasferire dati in assenza di una base giuridica ma, ad un tempo, sono consapevoli dell'enorme impatto che un blocco potrebbe avere sull'economia mondiale.

Il nesso tra protezione dati ed economia non è mai stato cosi evidente.

E mai è stata così chiara la necessità di un riconoscimento universale di questo diritto.

Del resto il diritto alla privacy, nato per garantire libertà e autonomia, nella dimensione digitale, per sua natura aterritoriale e per questo refrattaria ai confini di leggi e giurisdizioni, non può conoscere limiti e discriminazioni per nazionalità.

Non a caso, non solo in Europa, esso è considerato diritto fondamentale, come tale da riconoscere a prescindere dal requisito della cittadinanza.

Più efficaci, ma non meno liberi

L'Europa che nello stesso giorno approva tanto la nuova disciplina sulla protezione dati quanto quella sul PNR - che comprime sensibilmente tale diritto - deve vincere la tentazione di allontanarsi da se stessa e dai principi che la fondano: la garanzia della privacy, in particolare, come libertà dal controllo e condizione di una democrazia pluralista e personalista.

È anche per questo, per preservare la nostra autentica identità, che la reazione alla minaccia terroristica deve essere efficace ma rispettosa dei diritti e delle libertà fondamentali.

Ricordando che non tutte le limitazioni delle libertà sono effettivamente utili nella prevenzione del terrorismo o di gravi reati.

Soprattutto in un'epoca in cui il problema non è più tanto l'acquisizione dei dati quanto la capacità di analizzarli in modo efficace e selettivo, se è vero che gli autori delle ultime stragi erano tutt'altro che ignoti agli organi inquirenti.

La tecnica va dunque messa a servizio del diritto e non viceversa, senza illudersi di poter delegare a un algoritmo il successo delle investigazioni, che invece devono basarsi sempre sul fattore umano, capace esso solo di dare senso ai dati, altrimenti privi di ogni significato.

Se, come parrebbe potersi evincere dal caso Apple-FBI, esistono le chiavi per aprire non "tutte le casseforti" ma solo quella che può dare informazioni utili per gli inquirenti - con tutte le garanzie per l'interessato - essi devono poterne disporre.

E a richieste di acquisizione di dati puntuali e circostanziate per comprovate esigenze investigative, come quelle avanzate recentemente a Whatsapp dalla Procura di Milano, non può opporsi un'invocazione meramente strumentale della privacy.

Ma insieme, per converso, occorre difendere con rigore il sistema generale di criptazione senza il quale si affievolirebbero non solo le tutele per i singoli cittadini, ma le stesse difese nazionali dalla minaccia cibernetica.

Le tecniche d'indagine vanno dunque potenziate, ma utilizzate nella maniera più utile in termini di prevenzione e più sostenibile sotto il profilo democratico, avendo ben chiaro quale sia il grado di libertà cui si può rinunciare senza divenire schiavi del terrore e senza neppure abdicare a ogni diritto in nome della logica emergenziale.

Libertà del lavoratore e nuove tecnologie

L'uso della tecnica al servizio dei diritti e non in contrasto con essi è, del resto, un tema da affrontare anche in altri settori, cogliendo l'impatto che sulle libertà hanno strumenti cui deleghiamo la gestione di molta parte della nostra vita.

Il lavoro, in particolare, è terreno su cui l'evoluzione tecnologica sfida categorie giuridiche consolidate, costringendoci a ripensare gli equilibri su cui sinora hanno retto istituti essenziali.

Primo fra tutti quello Statuto dei lavoratori che, oltre quarant'anni fa, ha sancito l'intangibilità della sfera individuale del lavoratore, rispetto a controlli datoriali pervasivi.

Tentando di adeguare norme pensate per l'organizzazione fordista del lavoro alla realtà dei sistemi satellitari e della biometria, il Jobs Act ha apportato innovazioni rilevanti, pure in assenza di alcuni correttivi che noi avevamo suggerito.

Ma anche le nuove norme vanno interpretate alla luce del principio di proporzionalità riaffermato di recente dalla Corte europea dei diritti dell'uomo rispetto al controllo della mail aziendale in orario di lavoro.

La Corte ha ribadito che i controlli datoriali sono ammissibili soltanto se strettamente proporzionati e non eccedenti lo scopo di verifica dell'adempimento contrattuale, limitati nel tempo e nell'oggetto, previsti da preventive policy aziendali, mirati, mai massivi, e fondati su precisi presupposti.

Principi tutt'ora validi anche nel nostro ordinamento, così da garantire che i controlli sul lavoro siano improntati a gradualità nell'ampiezza e nella tipologia con assoluta residualità di quelli più invasivi.

Il principio di proporzionalità del controllo va del resto osservato anche rispetto alla discussa ipotesi delle telecamere in contesti particolari, a tutela di soggetti incapaci o in condizioni di particolare fragilità. È il caso, ad esempio, degli asili nido, ove il dibattito non si riferisce più al tradizionale conflitto tra

interessi datoriali e libertà del lavoratore ma investe invece il rapporto tra quest'ultima e la tutela dei bambini.

Interessando due diritti fondamentali il cui bilanciamento può assumere sfumature diverse, su questo tema potrebbe intervenire la legge, tracciando il confine tra l'autodeterminazione sul lavoro, spontaneità e immediatezza nella relazione educativa e protezione di soggetti particolarmente vulnerabili. Sempre, però, nel rispetto dei principi di minimizzazione e proporzionalità.

Salute e riservatezza, tra vecchie e nuove vulnerabilità

Il passaggio della pubblica amministrazione dalla dimensione materiale a quella digitale è una sfida con cui il nostro Paese deve misurarsi per coglierne le opportunità di sviluppo e competitività, ma anche per assicurare la più efficace garanzia dei diritti dei cittadini.

Cruciale in tal senso è la digitalizzazione della sanità, rispetto alla quale però la frammentazione, l'assenza di un piano organico di sicurezza e la disomogeneità che hanno segnato le prime esperienze, appaiono ancora più pericolose.

Perché la perdita, la sottrazione, l'alterazione di un dato sanitario mette a rischio banche dati essenziali e, insieme, viola quanto di più intimo vi è nella persona, esponendola a gravi discriminazioni.

Ma, soprattutto, la vulnerabilità del dato sanitario rischia di determinare errori diagnostici o terapeutici, con conseguenze anche letali.

La carente sicurezza dei dati e dei sistemi può rappresentare, in altri termini, una causa esiziale di malasanità mentre, per converso, la protezione dei dati e dei sistemi è un fattore determinante di efficienza sanitaria.

La tutela del paziente da queste nuove vulnerabilità dev'essere dunque un obiettivo centrale per un sistema sanitario in cui parallelamente alle opportunità crescono i rischi, tra moltiplicazione delle biobanche, servizi Cloud, assistenza sanitaria transfrontaliera, telematizzazione dei percorsi diagnostici, genomica e interoperabilità delle cartelle cliniche.

In questo senso, con i nostri provvedimenti abbiamo cercato di disciplinare una realtà nuova, superando l'asimmetria tra l'evoluzione della tecnica e la rigidità del diritto e delle sue formule.

Sui sistemi informativi della sanità si sono così coniugate esigenze di governo clinico e monitoraggio della spesa sanitaria con la protezione dei dati dei pazienti; su fascicolo e dossier sanitari elettronici si sono affermate (da ultimo con le Linee guida di giugno scorso) garanzie tali da assicurare al paziente tanto la riservatezza ed esattezza dei propri dati quanto la loro agevole utilizzabilità in percorsi terapeutici spesso complessi.

Un equilibrio importante si delinea nel rapporto tra analisi epidemiologica, ricerca medica e privacy dei pazienti.

Per quanto riguarda i registri di patologia ci siamo espressi sui provvedimenti approvati e su quelli in discussione in Parlamento, sottolineando soprattutto l'importanza della codifica reversibile.

Questa misura è, del resto, sancita dal nuovo Regolamento quale strumento necessario per coniugare le esigenze della ricerca biomedica ed epidemiologica con la riservatezza del paziente, la cui identificazione è possibile solo in caso di necessità. In questo, essenzialmente, la codifica reversibile si distingue dall'anonimizzazione tout court, che va invece assicurata rispetto ai trattamenti per fini statistici o amministrativi.

Privacy e media: un supplemento di responsabilità

Determinante è l'impatto che le nuove tecnologie, e soprattutto la rete, hanno sul rapporto tra riservatezza e diritto all'informazione.

Le caratteristiche di persistenza, riproducibilità, indicizzazione proprie delle notizie pubblicate sul web ne mutano profondamente effetti e natura, creando canali inediti di informazione dallo statuto giuridico spesso sfumato.

Significativa, in tal senso, è la decisione con cui abbiamo riconosciuto l'applicabilità ai blog d'informazione del regime peculiare sancito per i giornalisti,

negando quindi che costituisca illecito riportare, anche in assenza del consenso dell'interessato, notizie e commenti purché nel rispetto degli altrui diritti, libertà e dignità.

Rispetto cui lo stesso giornalista è sempre tenuto, nell'esercizio della responsabilità di coniugare, di volta in volta, esigenze informative e riservatezza individuale secondo il canone dell'essenzialità dell'informazione.

Questo parametro abbiamo più volte dovuto invocare, anche recentemente, a fronte della diffusione di un eccesso di dettagli inerenti la vita sessuale o comunque privata di soggetti, spesso anche vittime, coinvolti in inchieste giudiziarie: con il rischio di un accanimento informativo non utile ai cittadini e lesivo della dignità degli interessati, finanche indulgendo al sensazionalismo e al macabro su particolari relativi alla morte.

Nel caso, poi, della pubblicazione dei dati identificativi della vittima di una violenza sessuale, si è dovuto ricorrere al blocco per contenere i danni ulteriori in ragione della persistenza in rete della notizia.

Sotto un profilo solo in parte diverso - e comunque per proteggere tutti i soggetti coinvolti nei processi, a partire dalle vittime - sarebbe utile l'approvazione di una riforma del regime di pubblicità delle sentenze, che tenga conto degli effetti della loro pubblicazione in rete.

Come abbiamo suggerito più volte, sarebbe opportuno prevedere l'oscuramento, al momento della pubblicazione, dei nomi presenti nelle pronunce giurisdizionali, così coniugando esigenza di massima conoscenza del patrimonio giuridico contenuto nelle sentenze, trasparenza della giustizia e dignità delle parti e dei terzi.

Sul rapporto tra riservatezza dei soggetti a vario titolo coinvolti nei procedimenti giudiziari e diritto di informazione, alcuni effetti potranno derivare, sia pur indirettamente, dalle direttive di talune Procure volte a contenere - nel pieno rispetto del contraddittorio e del diritto di difesa - la trascrizione di intercettazioni inerenti aspetti irrilevanti ai fini delle indagini o terzi estranei.

Limitando così l'ingresso, nel fascicolo procedimentale, di dati personali non strettamente pertinenti al reato contestato, relativi a terzi o, comunque, dei quali si possa fare a meno senza per questo nuocere alle indagini: si potrebbe quindi evitare, a monte, il rischio di una loro indebita divulgazione sulla stampa.

È, questa, una strada già da noi auspicata e che ci auguriamo il legislatore possa percorrere, per garantire - nel rispetto dei diritti della difesa e della libertà di stampa - che negli atti processuali e, quindi, nella cronaca giudiziaria non siano riportati interi spaccati di vita privata - delle parti e, soprattutto, dei terzi - privi di reale rilevanza pubblica.

L'accesso universale e la parabola della trasparenza

Declinato spesso - ma non del tutto a ragione - in forma di ossimoro, il binomio trasparenza e privacy rappresenta uno dei temi di maggiore rilievo in un tempo, come il nostro, di crisi dei modelli politici, dell'idea di cittadinanza, degli stessi legami sociali.

L'affermazione del principio di "visibilità del potere" ha rappresentato in questo senso una risposta importante a un'istanza partecipativa e di sindacato diffuso sulla gestione della cosa pubblica, estendendosi da ambiti limitati sino a divenire forma dell'agire amministrativo.

La disciplina sulla trasparenza ha così subito una progressiva estensione, che ha portato a un'esigenza di razionalizzazione e ridefinizione degli obblighi di pubblicità, solo in parte colta dal recente decreto correttivo.

Esso non sviluppa infatti adeguatamente le potenzialità di alcuni criteri di delega, nel segno dell'efficacia, della selettività e della funzionalità ad obiettivi di controllo sull'esercizio del potere.

Non sono adeguatamente modulati gli obblighi di pubblicità in ragione del grado di esposizione del singolo organo al rischio corruttivo, della funzionalità del dato alle esigenze di trasparenza e del bilanciamento di tali esigenze con il diritto alla riservatezza degli interessati.

Diritto che viene ancor più compresso con l'istituzione dell'accesso

"universale", che diversamente da quello civico legittima chiunque ad accedere non solo ai dati soggetti a pubblicazione obbligatoria, ma ad ogni dato e documento ulteriore comunque detenuto da una pubblica amministrazione, salvo necessità di tutela di alcuni interessi tra i quali la protezione dati.

Nella sua genericità e in assenza di precisazioni o di una motivazione sottesa all'istanza, che orienti il bilanciamento cui è tenuta la pubblica amministrazione, tale parametro rischia di determinare interpretazioni eccessivamente discrezionali e differenziate, quando non addirittura arbitrarie, con conseguenze paradossali e violazioni di un diritto fondamentale quale appunto la protezione dati.

Per questo, sia in sede di audizione al Parlamento che di parere al Governo, abbiamo sottolineato l'esigenza di una più complessiva revisione della disciplina in attuazione dei suddetti criteri di delega.

Rispetto all'accesso universale e appunto sul modello del FOIA, abbiamo proposto l'oscuramento dei dati ove prevalga il diritto alla riservatezza e il divieto di comunicazione di dati di minori o comunque sensibili o giudiziari.

E questo, in conformità alla tutela rafforzata accordata a tali categorie di dati e secondo indicazioni puntuali da fornire con un apposito regolamento.

In assenza di tali precisazioni, si rischia infatti di oscillare, con irragionevoli disparità di trattamento, tra dinieghi ingiustificati e ostensioni di dati personali anche meritevoli della massima protezione. E la trasparenza è un istituto troppo importante per la nostra democrazia per prestarsi a una simile eterogenesi dei fini.

Cybercrime: una minaccia reale per la competitività delle aziende e la sicurezza dello Stato

La criminalità informatica ha assunto dimensioni inquietanti.

Sono oggetto di minacce credenziali e identità digitali di milioni di utenti e naturalmente la superficie di attacco cui siamo esposti aumenta in proporzione alla mole di dati disseminati nel web e più velocemente della nostra capacità di proteggerla.

Con lo sviluppo dell'Internet delle cose, poi, le vulnerabilità potranno estendersi sino a compromettere anche la sicurezza fisica delle persone.

Il peso attuale del cybercrime sull'economia mondiale viene stimato in 500 miliardi di euro all'anno, di poco al di sotto del narcotraffico nella classifica dei guadagni illeciti.

La logica conseguenza è la forma sempre più strutturata delle organizzazioni dedite a queste attività, che allo stato attuale offrono alti profitti con bassi rischi.

L'Italia nel 2015 ha subito un incremento del 30% dei crimini informatici, (+50% phishing, +135% ransomware) particolarmente rilevanti nel settore delle imprese.

Le tecniche di attacco utilizzate sfruttano una generale inadeguatezza delle misure di sicurezza adottate, a conferma di quanto denunciamo da tempo: la consapevolezza dei rischi crescenti non si accompagna ad una maggiore attenzione verso serie politiche di protezione dei dati e dei sistemi.

In tale contesto risulta davvero inspiegabile la refrattarietà di molte imprese a proteggere il loro patrimonio informativo, inserendo la sicurezza digitale tra gli asset strategici, assumendo la protezione dei dati quale nuovo fattore di vantaggio competitivo.

In questo ultimo anno sono quasi raddoppiate - 49 - le comunicazioni di data breach pervenute all'Autorità nel solo settore dei servizi di comunicazione elettronica.

Ma il cybercrime può avere un impatto devastante non solo in termini economici.

Sono sempre più diffusi fenomeni allarmanti di vere e proprie estorsioni e minacce fondate sul possesso di informazioni personali, spesso ottenute nell'ambito di relazioni "privilegiate" con la vittima.

In queste realtà la vittima, minore o meno, è ricattata o vessata da chi diffonda in rete sue informazioni o immagini intime o ne offenda in vario modo la dignità, davanti alla platea sconfinata della rete.

Questi fenomeni esigono non solo repressione ma soprattutto prevenzione, fondata in primo luogo sull'uso attento dei propri dati e la consapevolezza dell'importanza di proteggere, con essi, la nostra stessa persona.

Ed esigono un comune sforzo di tutti gli operatori della rete, anche oltre i confini della giurisdizione e la coercitività del diritto: importante, in questo senso, il codice di condotta concordato nel maggio scorso tra la Commissione Ue e i principali social network per il contrasto dell'hate speech.

Politiche pubbliche centrate sulla condivisione di dati

Anche la gestione delle politiche pubbliche risente della spinta a condividere sistemi e metodologie di analisi dei dati e da tempo la nostra Autorità accompagna lo sviluppo digitale del Paese con un'intensa attività consultiva.

Numerosi i pareri resi al Governo su temi fondamentali (quasi uno alla settimana!): dall'Anagrafe nazionale della popolazione residente, che ora conterrà anche l'archivio nazionale dei registri comunali di stato civile, alle modalità attuative dello SPID, dall'inserimento in bolletta del canone RAI all'amministrazione fiscale, al processo tributario telematico.

In particolare, per favorire l'innalzamento dei livelli di tutela delle banche dati pubbliche, anticipando le disposizioni del nuovo Regolamento, abbiamo prescritto anche a tutte le pubbliche amministrazioni l'obbligo di comunicare le violazioni o gli incidenti informatici eventualmente subiti.

Impegnativa è anche l'attività ispettiva e di vigilanza che ci consente di verificare il rispetto dei nostri provvedimenti prescrittivi.

In questo senso sono stati particolarmente utili gli interventi presso alcune tra le banche dati più grandi e strategiche del Paese.

È questa un'attività che intendiamo incrementare.

Il nostro impegno è costante affinché entrino a far parte delle buone pratiche di ogni pubblica amministrazione le misure di protezione dati: misure tecniche, informatiche, organizzative, logistiche e procedurali.

Un lavoro che si colloca nella prospettiva della nuova normativa europea che richiederà anche alla pubblica amministrazione un notevole salto di qualità nelle modalità di gestione dei dati.

Database interoperabili e pubbliche amministrazioni che si scambiano dati esigono, oltre alla sicurezza informatica, il rispetto delle garanzie di trasparenza verso i cittadini in merito agli obiettivi che si intendono perseguire e alle modalità per farlo.

I principi di finalità, pertinenza - quali ad esempio il divieto di estrarre dati in via automatica e massiva - e minimizzazione, ribaditi in tutti i provvedimenti adottati dall'Autorità, si dimostrano, unitamente alle rigorose regole tecniche, un presidio essenziale.

La legittimazione sociale degli obiettivi perseguiti, quali ad esempio la lotta all'evasione fiscale, è del resto più forte quando è percepita dai cittadini come rispettosa del loro diritto alla protezione dei dati.

Le pubbliche amministrazioni possiedono un patrimonio informativo di grande valore e in questo si inserisce l'obiettivo ambizioso di sbloccare completamente il potenziale dei dati in loro possesso.

Tuttavia le sfide degli open data, del riutilizzo delle informazioni del settore pubblico e delle capacità di analisi dei Big data richiedono non solo attenzione con riferimento alla sicurezza dei sistemi e delle infrastrutture utilizzate, ma la definizione di un ragionevole equilibrio tra valorizzazione del patrimonio informativo in mano pubblica e garanzia di tutela per i cittadini.

Per altro verso, aumentano in modo consistente le richieste di scambio di informazioni con altri Paesi e, in tale contesto, abbiamo partecipato a numerosi incontri in ambito OCSE al fine di definire un corretto scambio di dati fiscali.

Altrettanto rilevante l'attività svolta in seno al Consiglio d'Europa dove seguiamo attivamente il processo di revisione della Convenzione n. 108/1981.

Geolocalizzazione e biometria: scenari attuali di evolute attività di profilazione

A fronte della crescente diffusione di sistemi di riconoscimento biometrico che consentono effettive semplificazioni nelle nostre attività quotidiane (si pensi alla firma digitale nei documenti bancari ovvero alla possibilità di accedere agevolmente in determinati luoghi tramite l'impronta), abbiamo aggiornato la posizione del Garante, con un provvedimento generale e con successive ulteriori decisioni.

Consideriamo, tuttavia, condizione inderogabile che i principi di proporzionalità e minimizzazione siano sempre rispettati unitamente alla affidabilità dei sistemi utilizzati e alla integrità dei dati acquisiti, anche in considerazione delle riemergenti incertezze in merito all'effettiva riproducibilità dei dati biometrici.

Dati che, peraltro, il nuovo Regolamento ha equiparato a quelli sensibili, rafforzandone ulteriormente le tutele.

Per questo ci siamo opposti a forme generalizzate di raccolta di dati quali, in un caso recente, il riconoscimento facciale in assenza di stringenti misure di sicurezza.

Riteniamo necessario promuovere una maggiore consapevolezza dei rischi a fronte del sempre più diffuso ricorso ai sistemi di identificazione biometrica, in ogni circostanza e per qualunque finalità.

In questo senso sarà importante il nuovo obbligo, previsto dal Regolamento, di effettuare specifiche valutazioni di impatto privacy, prima dell'utilizzo di tali dati.

Aumentano le attività di localizzazione a fini di marketing, spesso con un basso livello di consapevolezza degli utenti rispetto a profilazioni sempre più analitiche e puntuali e, dunque, rischiose.

Nel valutare le diverse istanze di verifica preliminare, abbiamo anticipato alcune importanti misure introdotte dal nuovo Regolamento e richiesto adeguati

livelli di aggregazione dei dati, tecniche di pseudoanonimizzazione, sistemi automatici di cancellazione delle informazioni, soluzioni per impedire tracciamenti puntuali degli spostamenti degli utenti.

Elementi che permettono, in concreto, di trovare un giusto equilibrio tra la possibilità per le imprese di sfruttare il potenziale dei dati e la tutela degli interessati ai quali quei dati appartengono.

Positivo, perché coniuga le esigenze commerciali con il corretto uso di dati sull'affidabilità dei soggetti coinvolti, il Codice deontologico per le informazioni commerciali approvato dall'Autorità.

Il telemarketing: un nodo da sciogliere

Nel settore del telemarketing persistono le rilevanti criticità da tempo denunciate dal Garante e si continua a registrare un'incontenibile aggressività degli operatori che arriva a compromettere seriamente la tranquillità individuale e familiare.

Nel solo primo semestre del 2016 sono pervenute circa 3000 segnalazioni di telefonate promozionali ritenute illecite. Un numero spropositato che, al di là di ogni azione di contrasto, continua a crescere.

Abbiamo sollecitato nuovi e più efficaci interventi normativi tra i quali la possibilità di includere nel Registro delle opposizioni tutte le utenze, fisse e mobili, e non solo quelle presenti negli elenchi e sancire una più chiara responsabilità dei soggetti per conto dei quali viene effettuata la chiamata, anche in ragione della consolidata tendenza a subappaltare le attività, rendendo più difficili i dovuti controlli.

Mirati accertamenti ispettivi si stanno svolgendo in queste settimane nell'ambito di call center e aziende committenti, dai quali sembrano emergere gravi inadempimenti nella gestione dei dati.

Ma per preservare un settore produttivo, quale quello dei call center, oggi compromesso dal fenomeno del telemarketing "selvaggio", è indispensabile,

comunque, un supplemento di correttezza da parte degli operatori economici nonché una minore disinvoltura da parte degli utenti nel momento in cui manifestano il consenso all'uso dei propri dati.

Una transizione impegnativa

Nel 2015 abbiamo adottato 692 provvedimenti collegiali, inclusi ricorsi e pareri resi al Governo.

Sono circa 5000 i quesiti ai quali l'Ufficio ha dato risposta, 1696 le sanzioni contestate, 303 le ispezioni svolte anche con l'ausilio della Guardia di Finanza, cui siamo davvero molto grati.

Il nostro campo di azione è destinato a dilatarsi in ragione delle ulteriori funzioni che ci assegna il nuovo Regolamento.

Un consistente impianto sanzionatorio (fino al 4% del fatturato delle società), privacy officer, certificazioni dei sistemi, codici settoriali, notifica delle violazioni subite, portabilità dei dati, parere obbligatorio sulle norme primarie, meccanismi di Sportello unico per le imprese, sono alcuni tra i significativi adempimenti che obbligheranno a breve i soggetti privati e pubblici a ripensare tutte le loro attività in un'ottica pro-privacy.

Tra i settori di tradizionale intervento del Garante vale invece la pena richiamare quello di Autorità di controllo sulle banche dati nazionali del sistema Schengen e di informazione sui visti, che contengono dati di milioni di individui e che sono sempre più strategiche di fronte alle sfide migratorie alle quali siamo esposti.

Oggi più che mai al centro di un sistema europeo, il Garante ha già cominciato, in sinergia con le omologhe istituzioni europee, ad avviare i necessari cambiamenti.

E tuttavia non possiamo, in questa circostanza, non segnalare la strutturale sproporzione tra la vastità dei compiti assegnati alla nostra Autorità e le risorse umane e finanziarie disponibili.

E questo nonostante lo sforzo di un personale preparato e motivato che, unitamente al Segretario generale, desidero ringraziare.

Prima di concludere, consentitemi di ringraziare le Colleghe Augusta Iannini, Giovanna Bianchi Clerici, Licia Califano con le quali condivido quotidianamente, con grande armonia, impegni e responsabilità.