GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

A TUTELA DI UN DIRITTO FONDAMENTALE

Persona, diritti, innovazione

Discorso del Presidente

Antonello Soro

Relazione2016

Desidero innanzi tutto esprimere un particolarissimo ringraziamento al Presidente della Repubblica, che oggi ci onora della sua presenza, per l'attenzione con cui costantemente guarda alla nostra attività.

Ringrazio anche la Presidente della Camera per le sue parole e per l'ospitalità,

i rappresentanti del Governo e del Parlamento,

tutti i presenti.

Signor Presidente della Repubblica, Signora Presidente della Camera, Autorità, Signore e Signori,

L'8 maggio 1997 entrava in vigore nel nostro Paese la legge sulla tutela dei dati personali.

Nel corso di questi vent'anni quello che a qualcuno allora poteva apparire un istituto giuridico lontano dalla vita reale, ha invece influenzato, sempre più, scelte individuali e pubbliche, dimostrandosi un concretissimo presidio di libertà rispetto a forme di controllo tanto sottili quanto pervasive.

Da molti percepito in origine, riduttivamente, come mera rivendicazione dell'inviolabilità della sfera privata, tale diritto ha dimostrato, nel corso del tempo, le sue molteplici potenzialità: la sua capacità di difenderci da sempre nuove discriminazioni, di garantire la libera costruzione della personalità, la sovranità su di sé, sulla propria immagine e sul proprio corpo.

E questo anche per l'impegno profuso dai Componenti il Garante che ci hanno preceduto, ai quali va la nostra gratitudine.

Tutt'altro che presupposto di opacità e difesa di privilegi, il diritto alla protezione dei dati si è dimostrato un prezioso fattore di garanzia, capace di correggere quelle asimmetrie informative e disparità di forza contrattuale che caratterizzano, sempre di più, i rapporti tra i cittadini e i detentori del potere pubblico e privato.

E viene sempre più invocato di fronte a soverchianti "schiavitù volontarie" cui rischiamo di rassegnarci, in cambio di utilità e servizi digitali che paghiamo al prezzo di porzioni piccole o grandi della nostra libertà.

In un'epoca che di fronte alla tecnica sembra smarrire ogni senso del limite, proprio questo diritto rappresenta la bussola per riportare la persona al centro di uno sviluppo tecnologico altrimenti distopico e dispotico, per misurare l'innovazione anche secondo i criteri della sostenibilità sociale e dell'ammissibilità etica, prima ancora che giuridica.

Nella sua prima relazione al Parlamento, Stefano Rodotà si chiedeva

" .. se tutto quel che è tecnicamente possibile sia pure eticamente lecito, politicamente e socialmente accettabile, giuridicamente ammissibile".

Sono trascorsi vent'anni e la stessa sfida per noi si rinnova ogni giorno.

Da allora, certo, molto è cambiato.

Internet è divenuto il più grande e frequentato spazio pubblico che l'umanità abbia conosciuto, la nuova dimensione in cui si svolge una parte rilevante della nostra vita.

Il processo di trasformazione digitale investe la maggior parte delle relazioni tra le persone e tra queste e le pubbliche amministrazioni e le imprese.

L'interconnessione di oggetti, sensori, dispositivi di uso quotidiano, alimenta il trattamento di grandi volumi di dati e favorisce applicazioni sempre più stupefacenti dell' intelligenza artificiale, destinate a cambiare in profondità i processi economici e l'organizzazione sociale.

Una nuova categoria di tecnologie, che utilizza l'elaborazione del linguaggio naturale e dell'auto apprendimento, potrà consentire alle persone e alle macchine di interagire in modo più naturale, accrescendone competenze e capacità cognitive.

La relazione tra mercato e diritti si gioca su questo terreno.

E nell'epoca della disintermediazione e delle post-verità, nuove sfide complicano ulteriormente la tenuta e il senso della democrazia.

Dopo l'11 settembre il rapporto tra libertà e sicurezza si modula su equilibri ben diversi da quelli di vent'anni fa e in questi anni ci si è addirittura chiesti, se la prima possa sopravvivere al terrorismo.

Ma la privacy è nome della libertà e le esperienze ci dicono che, fronte alle nuove minacce, essa sia non soltanto possibile, ma addirittura indispensabile per rendere le attività di contrasto più risolutive, perché meno massive e quindi orientate su più congrui bersagli. Per far sì che nella lotta al terrorismo, siamo più efficaci, non meno liberi.

Il contesto in cui oggi ci muoviamo e in cui opera il Garante, quale unica Autorità preordinata non già alla regolazione di uno specifico settore, ma alla tutela di un diritto fondamentale in qualsiasi ambito della vita è, dunque, assai diverso da quello in cui si inseriva il Garante al momento della sua istituzione.

Ma, nel differente contesto, quella della protezione dati è ora - come e più di allora - la frontiera su cui si gioca una parte rilevante del nostro futuro.

Lo è più di allora perché oggi, assai più che vent'anni fa, non vi è attività privata o pubblica che non si fondi su tecnologie alimentate da dati personali.

Le telecamere - che vent'anni fa iniziavano a diffondersi nelle nostre città - sono oggi non solo molto più numerose, ma anche più "intelligenti": riconoscono le persone, classificano i comportamenti e reagiscono di conseguenza.

I processi di automazione del lavoro ne stanno determinando quasi una de-umanizzazione.

La progressiva sostituzione dei lavoratori - anche di quelli addetti alle funzioni più complesse - con le macchine, è destinata ad avere conseguenze sociali rilevantissime.

Anche gli sforzi più encomiabili fatti in tale campo per presidiare con adeguate garanzie l'incessante evoluzione - si pensi ai tentativi dell'Unione europea di definire lo statuto giuridico dei robot - mostrano quanto il diritto fatichi a tenere il passo di queste trasformazioni e delle sfide che essi pongono, non solo in termini responsabilità.

A breve - annunciano i ricercatori - nuove tecnologie consentiranno al cervello di scrivere e alla pelle di ascoltare, attraverso dispositivi indossabili.

L'intelligenza artificiale, dunque, viene spinta sino al punto di mutare la stessa funzione dei nostri organi.

La combinazione tra informatica e genetica ha consentito alla tecnologia di insinuarsi fin nelle pieghe più profonde delle nostre esistenze, riscrivendone codici, sovrapponendo biologia e biografia.

La progressiva mappatura dell'intero patrimonio genetico ha reso evidenti le potenzialità straordinarie della medicina predittiva e di precisione, il cui sviluppo non può prescindere, tuttavia, da un'adeguata tutela delle informazioni personali sulle quali si basa.

Abbiamo approfondito il tema in occasione dell'ultima giornata europea.

E anche prescindendo dagli sviluppi futuri, il nostro processo già oggi non è immune dalla tentazione della delega fideistica della giurisdizione alla scienza che, per quanto esatta, non conosce i parametri della responsabilità, della colpa e dell'equità. La delega all'algoritmo persino della prognosi di recidiva penale, oggetto di recente controversia in alcuni stati americani, è in tal senso significativa.

In un contesto di così incessante cambiamento, garantire il diritto alla protezione dei dati personali vuol dire coniugare tecnologia e umanità, libertà e sicurezza, trasparenza del pubblico e riservatezza del privato, informazione e dignità, iniziativa economica e autonomia individuale, scienza e libertà dal determinismo.

La libertà e i suoi nuovi confini

E se oggi, più di vent'anni fa, la protezione dei dati è condizione necessaria per la libertà e la democrazia, è anche e soprattutto perché la nostra più effettiva dimensione di vita è, paradossalmente, quella digitale. Densa di straordinarie opportunità, ma anche di insidie.

Perché i dati costituiscono la proiezione digitale delle nostre persone e insieme ne manifestano la vulnerabilità.

Al web affidiamo dubbi, speranze e timori espressi non solo da commenti e immagini sui social network ma anche, più semplicemente, dalle tracce della nostra attività in rete.

Internet è divenuto la nuova dimensione entro cui si svolge - per citare l'articolo 2 della Costituzione - la personalità di ciascuno: è la realtà in cui i diritti si esercitano o possono essere negati, le libertà si dispiegano o sono violate.

L'assenza di limiti, propria della rete, ha offerto infinite potenzialità di crescita e conoscenza, alle quali meno frequentemente si è accompagnato un corrispondente esercizio di consapevolezza e responsabilità. Se sul web la libertà si esprime in ogni sua potenzialità anche la violenza, specularmente, non conosce limiti.

Dalla violenza verbale da parte di chi, in rete, supera ogni freno inibitorio erroneamente confidando nell'anonimato, fino alle aberrazioni di Blue Whale e all'esibizione online di atti omicidi, in un crescendo di lucidissima follia.

Per altro verso, il passaggio all'Internet delle cose, che rende gli oggetti comuni strumenti di connessione interattiva, ha digitalizzato ogni aspetto della vita quotidiana, moltiplicando esponenzialmente il volume dei dati trattati non sempre con adeguate garanzie, come dimostrano i tanti attacchi dei quali sono vittime imprese e amministrazioni anche italiane.

La combinazione tra la tendenza, sempre più diffusa, alla condivisione e la centralità dei Big Data per il sistema economico, costituisce il fondamento dell'economia digitale, basata sullo sfruttamento commerciale delle informazioni personali e sulla costruzione di modelli identitari omologati e omologanti, per condizionare scelte individuali e collettive.

L'identità personale rischia così di ridursi ad un profilo di consumatore, elettore, comunque utente che un algoritmo attribuisce a ciascuno, finendo per annullare l'unicità della persona, il suo valore, la sua eccezionalità. L'identità personale diventa una cifra per Big Data.

La tutela della persona rispetto a queste forme di monitoraggio più o meno occulto del proprio comportamento in rete, è dunque indefettibile garanzia di libertà.

Del resto, se ciò che per ciascuno è dato personale, intima essenza del sé, diviene per i grandi monopolisti del web dato economico da sfruttare commercialmente, le implicazioni in termini antropologici, ma anche sociali e politici sono eloquenti.

E' significativo che la legislazione europea in materia ruoti attorno alla figura del "data subject": l'interessato è definito a partire dai suoi dati, ne è fonte ed allo stesso tempo ne ha la signoria, il cui esercizio rappresenta la vera e unica garanzia rispetto ai tanti "grandi fratelli" che governano la rete.

La concentrazione in capo a pochi soggetti privati di un rilevantissimo potere, non solo economico, ha infatti determinato un mutamento sostanziale nei rapporti tra individuo e Stato, tra pubblico e privato, cambiando profondamente la geografia del potere.

Un numero esiguo di aziende possiede un patrimonio di conoscenza gigantesco e dispone di tutti i mezzi per indirizzare la propria influenza verso ciascuno di noi, con la conseguenza che, un numero sempre più grande di persone - tendenzialmente l'umanità intera - potrà subire condizionamenti decisivi.

Gli Over the Top sempre più spesso intervengono, in un regime prossimo all' autodichia, per comporre istanze di rilevanza primaria, quali informazione e diritto all'oblio, libertà di espressione, dignità e tutela dalle discriminazioni, veridicità delle notizie diffuse. E, ad un tempo, assumono un ruolo da protagonisti in campi anche molto lontani dalla loro vocazione originaria, dalla finanza alla genetica, dall'automazione alla realtà aumentata.

Parallelamente, l'intervento statale è reso più complesso dalla capacità delle nuove tecnologie di scardinarne i presupposti essenziali: in primo luogo la territorialità, quale criterio di competenza ed applicazione della legge.

Il nuovo quadro giuridico europeo

La misura delle nostre libertà è, dunque, fortemente condizionata dall'operato delle grandi imprese dell'economia digitale.

In questo scenario interviene il nuovo quadro giuridico europeo in materia di protezione dati (regolamento generale e direttiva inerente i settori di giustizia e polizia) da poco più di un anno pubblicato in Gazzetta ufficiale e tra poco meno di un anno applicabile negli Stati membri (con l'intermediazione della normativa di recepimento per la direttiva).

A questi si aggiungerà fra breve il nuovo, specifico regolamento sulle comunicazioni elettroniche.

Nato dall'esigenza di evitare quel rischio di anacronismo che corre sempre il diritto nel suo rapporto con la tecnologia, il regolamento generale sulla protezione dati conia una disciplina uniforme e direttamente applicabile nel territorio dell'Unione, così da superare le asimmetrie tra ordinamenti, rese possibili dal recepimento non del tutto omogeneo della direttiva 95/46/CE.

Estende inoltre il proprio ambito di applicazione anche ai soggetti stabiliti al di fuori dell'Unione, superando così disparità di trattamento inaccettabili anche sotto il profilo concorrenziale, rispetto a operatori europei che offrono i medesimi servizi.

Questo è, del resto, il portato di una giurisprudenza che ha sempre più tentato di superare lo schermo dei confini nazionali per garantire un'adeguata tutela a un diritto, quale quello alla protezione dati che, poiché fondamentale, pertiene alla persona in quanto tale, a prescindere da ogni altro requisito.

Proprio l'esigenza di assicurare ai cittadini europei una tutela adeguata anche rispetto a chi ne trattasse i dati oltreoceano, aveva indotto la Corte di giustizia ad annullare il Safe Harbour, recentemente sostituito da un nuovo accordo sul trasferimento dei dati: il Privacy Shield.

In applicazione del nuovo accordo il Garante ha già autorizzato il trasferimento di dati negli Usa, riservandosi di effettuare verifiche sulla correttezza delle operazioni realizzate.

Tuttavia le prime scelte adottate in materia dalla nuova Amministrazione degli Stati Uniti, in contrasto con quella precedente, rischiano di riallargare lo iato tra Europa e Stati Uniti.

Ma quel rigore, doverosamente utilizzato dalle autorità di protezione dei dati europee per valutare il sistema di garanzie statunitensi, deve imporci di utilizzare gli stessi parametri in tutti gli altri contesti, a partire dalla valutazione dei trasferimenti di dati verso la Cina, conseguenti alla crescente presenza nel mercato europeo degli operatori di tale Paese.

Dovremo batterci per promuovere uno scudo privacy anche con la Cina. Soprattutto in ragione dell'evoluzione che ha caratterizzato il modello europeo, con il regolamento emancipato dalla dimensione riduttiva del mercato interno, in favore del più ampio approccio di tutela di un diritto fondamentale, sancito come tale dai trattati e dalla Carta di Nizza.

E concepire la protezione dati quale punto d'incidenza di molteplici diritti e libertà non può che avere implicazioni importanti.

In primo luogo, la scelta di un modello giuridico di tutela fondato sul ruolo di garanzia di autorità indipendenti, sempre più partecipi di una rete istituzionale di matrice europea.

Rilevante, in questo senso, non solo il rafforzamento delle forme di cooperazione tra autorità nazionali, ma anche il ruolo attribuito - con funzioni non solo consultive ma anche dispositive - al Comitato europeo per la protezione dei dati (l'European Data Protection Board), all'interno del quale il Garante siederà a fianco delle altre autorità europee.

Dall'approccio orientato ai diritti deriva anche il passaggio da una tutela in chiave prevalentemente remediale, dunque successiva, a una di tipo essenzialmente preventivo. Fondata, come tale, sulla minimizzazione del rischio di violazione attraverso tecniche di protezione fin dalla progettazione e con impostazioni predefinite ma anche mediante la complessiva responsabilizzazione dei titolari del trattamento, nella prevenzione del rischio "sociale" derivante da banche dati poco protette.

E se il contesto normativo italiano in cui le norme europee si innesteranno offre già oggi significative garanzie, ciò su cui invece si dovrà puntare è un investimento - non solo in termini economici ma anche istituzionali, politici, culturali - nella protezione dati.

Essa appare sempre di più una risorsa strategica di sviluppo e addirittura di sicurezza complessiva del Paese, fattore abilitante e di competitività, dunque da assicurare non già per mero obbligo di legge o adempimento burocratico, ma nell'interesse di tutti.

L'implementazione del regolamento necessiterà, dunque, prima di tutto di un mutamento culturale da parte di amministrazioni e imprese, cittadini e Stato, affinché la protezione dati sia considerata non già un costo, ma la risorsa essenziale in una società sempre più digitale e interconnessa.

Banche dati, algoritmi e sicurezza

Ciascuno di noi è conosciuto quasi esclusivamente attraverso i dati che lo riguardano, detenuti in banche dati, pubbliche e private, nelle quali l'identità è frammentata in ragione della particolare tipologia di sistema informativo in cui è inserita.

Di qui l'importanza di garantire l'esattezza, l'aggiornamento, la pertinenza dei dati trattati in modo da scongiurare il rischio di classificazioni errate e distorsioni di tratti importanti dell'identità individuale, sfuggendo alla tentazione di delegare tutto alla tecnologia.

In ogni caso è necessaria un'adeguata trasparenza sul funzionamento dei meccanismi di decisione automatizzata.

Sui limiti intrinseci che presentano tali decisioni è basato il provvedimento con cui abbiamo dichiarato illegittima l'ipotizzata costituzione di una banca dati per la misurazione del "rating reputazionale".

In quel caso una questione complessa come la reputazione, sotto il profilo professionale ed economico, sarebbe stata ridotta a mero calcolo svolto da un software, in base a dati reperiti in rete o caricati dagli stessi interessati dietro la pressione delle conseguenze negative altrimenti preconizzate.

Al di là del fatto che affidare ad un algoritmo la "recensione" di una persona al pari di un prodotto commerciale, aprirebbe una deriva davvero pericolosa, tale sistema avrebbe presentato un rischio elevato di attribuire agli interessati profili deformati della loro reale identità, con danni irreparabili per la dignità e la vita sociale e lavorativa degli stessi.

In questi anni la sottrazione di dati personali nel web, a scopo di frode, ha registrato una crescita smisurata: spesso per realizzare, attraverso il furto di identità, ulteriori crimini.

E' il caso di un' importante operazione di riciclaggio nel settore del money transfer, rispetto alla quale abbiamo irrogato una sanzione di 11 milioni di euro.

Anche quest'anno l'Autorità ha profuso un grande impegno in relazione al governo delle banche dati pubbliche e private, in ragione dell'importanza che assumono la sicurezza e la qualità dei dati per evitare inefficienze e procedure decisionali viziate, pregiudizievoli per l'affidabilità di enti pubblici e privati e per la stessa funzionalità della pubblica amministrazione e del mercato.

Significativo il provvedimento con cui, al termine di una complessa attività ispettiva, si sono accertate gravi criticità, da parte di un grande operatore telefonico, nell'integrità e qualità delle proprie banche dati (perfino quella sul traffico telefonico a disposizione dell'autorità giudiziaria), che hanno determinato l'assegnazione indebita di utenze a un numero consistente di clienti ignari.

Deve essere inoltre segnalata la condotta omissiva tenuta dalla Società, durante un assai ampio arco temporale, anche successivo alla segnalazione.

Con riserva dei successivi provvedimenti sanzionatori, abbiamo prescritto una ricognizione generale dei sistemi, insieme a verifiche puntuali e misure organizzative volte a consentire controlli preventivi e correzioni tempestive delle anomalie riscontrate.

In un caso recente, relativo ad altro operatore, un attacco informatico effettuato sfruttando una vulnerabilità dei sistemi, ha consentito l'accesso, con successiva copia, alle credenziali di autenticazione di oltre 5.000 clienti, utilizzate per accedere all'area riservata delle proprie utenze.

La sola acquisizione delle credenziali di accesso, infatti, è da considerare, già di per sé, fonte di potenziale pregiudizio per gli interessati, con particolare riferimento al rischio di furto d'identità, indipendentemente dal fatto che vi sia un loro effettivo utilizzo nel medesimo contesto, giacché spesso gli utenti adoperano le stesse credenziali per accedere a diversi servizi web.

Per quanto concerne le grandi banche dati pubbliche, all'esito di verifiche ispettive e di accertate vulnerabilità, abbiamo prescritto all'Agenzia delle Entrate un incremento dei livelli di sicurezza rispetto all'Anagrafe tributaria.

Ci siamo anche adoperati per garantire, rispetto alla dichiarazione dei redditi precompilata, maggiore sicurezza nell'accesso degli intermediari e nella trasmissione delle informazioni all'Agenzia delle Entrate, assicurando la non eccedenza dei dati raccolti e definendo i tempi di conservazione.

Riguardo alla riscossione del canone Rai abbiamo richiesto l'utilizzo di dati esatti, e non solamente presuntivi, per identificare i soggetti ai quali può essere addebitato in bolletta e individuato modalità semplici per informare gli utenti.

E' in corso la verifica dell'attuazione dello SPID, per valutare l'idoneità delle procedure di attribuzione dell'identità digitale e dei livelli di sicurezza per l'accesso ai servizi offerti online.

Un'attenzione particolare è stata rivolta anche alle banche dati nel settore della sanità, il cui valore anche economico è enorme, come tra l'altro dimostrano gli investimenti stimati dalla creazione a Milano di un

centro di ricerca europeo, rispetto al quale l'Autorità vigilerà per contemperare libertà della ricerca scientifica e tutela dei diritti dei pazienti.

Sempre nel settore sanitario, il Garante ha profuso uno straordinario impegno partecipando attivamente al tavolo di lavoro sul Fascicolo sanitario elettronico, fornendo tutte le indicazioni necessarie a consentire la piena attuazione di questa importante innovazione a beneficio dei cittadini.

La resilienza informatica e quella della democrazia

Nelle scorse settimane l'attacco informatico attraverso Wanna Cry ha ingenerato allarme in tutto il mondo.

Non sarà purtroppo l'ultimo. Nella dimensione digitale si svolgono, sempre di più, le relazioni ostili tra gli Stati e dentro gli Stati.

Secondo stime recenti, nello scorso anno le infrastrutture critiche sarebbero state oggetto del 15 per cento di attacchi in più rispetto al precedente e sarebbero cresciuti del 117 per cento quelli riconducibili ad attività di cyberwarfare, volte a utilizzare canali telematici per esercitare pressione su scelte geopoliticamente rilevanti.

Nel 2016 gli attacchi informatici avrebbero causato alle imprese italiane danni per nove miliardi di euro ma meno del 20 per cento delle aziende farebbe investimenti adeguati per la protezione del proprio patrimonio informativo. Il settore pubblico non risulta essere molto più efficiente.

Per questo la sicurezza dei dati deve rappresentare un fattore abilitante per soggetti privati e pubblici, da perseguire fin dalla progettazione dei sistemi e delle infrastrutture.

La resilienza informatica nel contrasto delle minacce cibernetiche deve, dunque, rappresentare ciò che la resilienza della democrazia rappresenta nel contrasto del terrorismo.

E per garantire davvero la cybersecurity - componente strategica della sicurezza nazionale e pubblica - è necessario evitare il rischio della parcellizzazione dei centri di responsabilità, con una centralizzazione di competenze e un'organica razionalizzazione del patrimonio informativo, anzitutto pubblico.

Ciò vale tanto per i Big Data di cui si alimenta la pubblica amministrazione, quanto per la "signal intelligence" e in generale l'attività d'indagine di tipo strategico, che rischia di allontanarsi da quel principio di proporzionalità tra privacy ed esigenze investigative ribadito più volte dalla Corte di giustizia.

E di recente declinato così da tradurre uno strumento investigativo ontologicamente massivo, quale la data retention, in uno selettivo, da applicare a obiettivi mirati e in base a presupposti stringenti.

La proporzionalità dei dati trattati rispetto alle esigenze investigative è, del resto, un criterio che ha contraddistinto le indicazioni fornite dal Garante, in particolare, attraverso pareri sui decreti attuativi della riforma della disciplina dei trattamenti per fini di polizia.

Nello specifico, in ragione delle minori garanzie accordate all'interessato in questo settore, abbiamo richiesto di circoscrivere i relativi trattamenti, escludendovi quelli svolti per finalità amministrative,

nonché, di limitare i tempi di conservazione a quanto strettamente necessario per le finalità investigative perseguite, soprattutto rispetto ai dati di persone nei cui confronti non siano emersi indizi significativi.

Analogamente, sono state previste maggiori garanzie relativamente alla banca nazionale del DNA, per la cancellazione dei dati, in particolare genetici, riferibili a soggetti assolti, in linea con i principi della direttiva 680/2016.

Giustizia e protezione dati

Rispetto alla cronaca giudiziaria si è registrata, anche quest'anno, la diffusione di atti d'indagine in violazione del relativo regime di pubblicità e spesso anche del principio di essenzialità dell'informazione.

Mai come in quest'ambito occorre un impegno comune.

Giustizia e informazione si caratterizzano principalmente, infatti, per la loro indipendenza e, quindi, per la responsabilità nell'esercizio delle rispettive funzioni. Responsabilità tanto più necessaria rispetto al potenziale distorsivo del processo mediatico, in cui logica dell'audience e populismo penale rischiano di rendere la presunzione di colpevolezza il vero criterio di giudizio.

Tale esercizio di responsabilità sarà certo favorito dalla proficua circolarità instaurata tra giurisdizione, organo di governo autonomo della magistratura e Garante, al fine di coniugare esigenze di giustizia e privacy. In particolare riguardo al tema delle intercettazioni, su cui diverse Procure e Csm hanno adottato provvedimenti volti a limitare - nel rispetto del contraddittorio e del diritto di difesa - la trascrizione di contenuti inerenti aspetti irrilevanti ai fini delle indagini o terzi estranei.

Molte delle indicazioni contenute in tali provvedimenti e conformi alle raccomandazioni da noi espresse più volte, sono state trasfuse in criteri di delega nella riforma penale all'esame del Parlamento.

E va certamente regolamentato l'utilizzo dei captatori a fini intercettativi (i cosiddetti trojan horse), definendo con rigore il perimetro delle garanzie, in ragione della strutturale diversità di tale strumento investigativo rispetto a quello normato dal codice di rito.

E' peraltro indispensabile selezionare i fornitori di servizi di intercettazione in base alle garanzie di sicurezza del trattamento offerte.

L'esternalizzazione di diverse operazioni investigative rende, infatti, assai più permeabile la filiera su cui si snoda l'attività captativa, meritevole per ciò di una tutela rafforzata, come dimostrano anche alcune istruttorie aperte dal Garante su tale fronte.

Significativa, in tal senso, la sanzione irrogata a un consulente tecnico dell'autorità giudiziaria che aveva illegittimamente conservato un archivio di dati personali di notevoli dimensioni, costituito inizialmente per fini di giustizia. Aveva altresì illegittimamente messo a disposizione di numerosi soggetti, compresi alcuni giornalisti, atti giudiziari acquisiti nel corso della sua attività.

Solo l'adozione di adeguate misure di sicurezza, da parte di ciascun soggetto coinvolto in ogni fase dell'indagine, può contribuire a minimizzare i rischi inevitabilmente connessi alla frammentazione dei

centri di responsabilità, derivanti dal coinvolgimento di soggetti diversi nella catena delle attività investigative.

Per quanto concerne la disciplina della pubblicazione telematica dei provvedimenti giurisdizionali, pur non essendo stata approvata la relativa riforma, si sono tuttavia registrate sul punto significative innovazioni, anche nel solco della positiva interlocuzione realizzata dal Garante con gli organi competenti.

Lavoro, telemarketing, trasparenza amministrativa

Particolare attenzione abbiamo riservato alle garanzie per il trattamento dei dati personali nel contesto lavorativo.

Fra i tanti casi esaminati, si può ricordare quello di un Ente che verificava illecitamente, in forma indiscriminata, gli accessi del personale alla rete e alle e-mail, utilizzando software operanti con modalità non percepibili dall'utente. Tali programmi - non potendo considerarsi "strumenti utilizzati (…) per rendere la prestazione lavorativa" - avrebbero dovuto determinare l'attivazione delle garanzie previste per i controlli a distanza.

E in ogni caso, si sarebbero dovute privilegiare misure graduali tali da rendere assolutamente residuali i controlli più invasivi, legittimati solo in presenza di specifiche anomalie.

Per quanto concerne il settore del telemarketing, nel 2016 le segnalazioni sono state circa 6000.

L'attività ispettiva dell'Autorità, svolta con l'ausilio del Nucleo speciale privacy della Guardia di finanza, che ringrazio per la consolidata essenziale collaborazione, ha messo in luce rilevanti illeciti commessi da primarie società di telefonia (milioni i dati trattati in violazione di legge) e si è concretizzata in importanti provvedimenti prescrittivi e sanzionatori. Anche recentemente confermati dal giudice ordinario.

L'attività di accertamento in loco si è svolta anche presso alcuni call center albanesi nella cornice del protocollo stipulato nel 2015.

In termini più generali, dagli elementi in corso di acquisizione, si rileva che con crescente frequenza dovrà richiedersi la collaborazione di altre autorità di controllo, sia nel territorio dell'Unione (Romania e Bulgaria), sia al di fuori di esso (Albania e Svizzera).

Abbiamo quindi suggerito al legislatore modifiche normative tali da rafforzare le garanzie dei cittadini e contrastare, in particolare, le condotte elusive della disciplina fondata sul consenso.

Il disegno di legge di riforma di tale disciplina, all'esame del Senato, ha raccolto alcune di queste indicazioni e, ove superati gli effetti contraddittori di una norma contenuta nel d.d.l. concorrenza, potrebbe condurre verso un governo più efficiente del settore.

Un impegno costante e notevole ha comportato l'implementazione della disciplina della trasparenza amministrativa comprensiva, tra l'altro, dell'accesso civico generalizzato.

L'assenza di motivazione delle istanze di accesso e la lacunosità dei parametri offerti dalla legge, ai fini della valutazione delle richieste, ha reso evidente il rischio di un'applicazione della nuova disciplina, oscillante tra un'eccessiva rigidità interpretativa e, all'opposto, una dilatazione ingiustificata della nozione di trasparenza.

A rischi del genere tentano di ovviare le indicazioni fornite con le linee guida dell'Anac adottate - pur in un testo sicuramente perfettibile - con la nostra intesa e suscettibili di revisione dopo un anno di applicazione.

Un elemento di garanzia del sistema è rappresentato dal parere del Garante sul ricorso o il riesame, avverso il diniego o il differimento dell'accesso per ragioni di tutela della riservatezza.

Le numerose richieste di parere, cui per legge dobbiamo rispondere entro il termine di 10 giorni sta comportando, per il personale del Garante, un impegno ai limiti della sostenibilità.

La libertà di espressione tra oblio, fake news, odio informativo

Il diritto all'oblio continua ad essere un terreno di confronto importante nel rapporto tra protezione dati e informazione, promosso dalle istanze che i cittadini ci rivolgono, con sempre maggiore frequenza e consapevolezza.

In quest'ambito, ci è stato possibile tracciare alcuni criteri importanti per coniugare memoria collettiva e dignità della persona.

In particolare, si è chiarito come anche una rilevante distanza temporale non possa, di per sé sola, legittimare la deindicizzazione di notizie inerenti reati particolarmente efferati che - come nel caso del terrorismo interno - abbiano segnato la storia del Paese.

Per altro verso, si è ritenuto sussistente il diritto alla rimozione, dai risultati di ricerca, di notizie che, in quanto superate dagli eventi successivi, non possano più ritenersi esatte.

Costante è stata l'attenzione al rapporto tra libertà di espressione e protezione dei dati personali nel contesto dei social network, anche rispetto alle varie forme di sfruttamento, persino commerciale, dei dati sulla vita privata degli utenti lì contenuti.

In diverse occasioni ci siamo attivati per bloccare la diffusione dei dati.

Come nel caso recente delle donne di Monza e Lecco, i cui profili Facebook sono stati riversati, a loro insaputa, in un, "catalogo delle single", esibite come prodotti in vetrina.

Abbiamo poi chiarito come l'anonimato da accordarsi ai minori coinvolti a qualsiasi titolo in procedimenti giudiziari, vada garantito a prescindere dalla natura aperta o meno del profilo.

E' un principio suscettibile di applicazione anche al di là del caso esaminato, per la difficoltà di circoscrivere, sui social network, i potenziali destinatari delle comunicazioni; in ragione dell'agevole modificabilità della natura, aperta o chiusa, dei profili e della possibilità per qualunque "amico" di condividere sulla propria pagina il post rendendolo, così, visibile ad altri soggetti, potenzialmente infiniti.

E dai rischi insiti nella naturale tendenza alla diffusività e alla propagazione in rete, di notizie lesive della dignità dei minori, muove la legge sul cyberbullismo.

Particolarmente positiva è la scelta di coniugare un approccio preventivo e riparatorio, grazie alla promozione dell'educazione digitale e alla specifica procedura di rimozione dei contenuti lesivi presenti in rete.

Il meccanismo delineato evita una preventiva e generalizzata ingerenza da parte dei provider e tuttavia li responsabilizza su segnalazione degli interessati, anche se minori.

L'Autorità si impegna a svolgere l'importante funzione di garanzia assegnatale dalla legge, nella consapevolezza sia delle oggettive difficoltà tecniche sia della necessità di risorse adeguate ai nuovi compiti.

Per altro verso, secondo recenti ricerche, la pedopornografia in rete e, particolarmente nel dark web, sarebbe in crescita vertiginosa: nel 2016 due milioni le immagini censite, quasi il doppio rispetto all'anno precedente.

Fonte involontaria sarebbero i social network in cui genitori postano le immagini dei figli.

E tra i rischi di un uso distorto del web e di una certa tendenza all'autismo informativo - per cui si tende a ricercare, in una spirale auto confermativa, le notizie che rafforzano le nostre convinzioni - vi è anche quello delle fake news.

Definizione attribuita a cose molto diverse tra loro (falsità, tweet automatizzati, hate speech, veri attacchi cibernetici), accomunate dalla tendenza a far dipendere l'attendibilità della notizia non dalla sua verificabilità, ma dalla quantità di condivisioni ottenute.

Diversi social network hanno sviluppato strumenti per aiutare gli utenti a verificare le informazioni presenti sulla loro piattaforma e contrastare le bufale virali.

E diverse soluzioni sono state proposte anche in sede politica.

Su questo terreno penso che non siano risolutive né la via esclusivamente tecnologica - che automatizzando il riscontro fattuale deprimerebbe ulteriormente il senso critico - né quella penale, che finirebbe con l'assegnare alla magistratura il ruolo di Tribunale della Verità.

Laddove in democrazia l'esattezza non è conseguibile altrimenti che con il pluralismo dialettico. Ferme restando le norme anche penali a tutela della dignità, che delimitano il confine oltre il quale la libertà di espressione non può spingersi.

E' illusorio pensare che possano esistere nuove autorità od organi certificatori della verità.

Il fenomeno delle fake news e l'uso distorto del web che ne è alla base vanno contrastati con una strategia complessa e articolata, ma non per questo meno energica.

A partite da un forte impegno pubblico e privato nell'educazione civica alla società digitale e al pensiero critico, dalla sistematica verifica delle fonti e da una forte assunzione di responsabilità da parte di ciascuno: dal singolo utente alle redazioni e, certo, ai grandi gestori della rete, con le loro tecnologie e le loro grandi risorse.

Perché la democraticità dell'infosfera è una risorsa che tutti dobbiamo preservare.

Gli effetti prodotti anche in campo politico-elettorale da tali fenomeni, in occasione delle competizioni elettorali di grandi democrazie come gli Stati Uniti o la Francia inducono a ritenere urgente anche una più complessiva riflessione sull'aggiornamento della ormai datata disciplina delle campagne elettorali, con riferimento ai mezzi di comunicazione politica oggi più frequentemente utilizzati.

Nuove sfide, impegni crescenti, risorse necessarie

Ci troviamo in un contesto di grande cambiamento sul versante normativo, che incide in modo significativo sul funzionamento e sui compiti dell'Autorità. Oltre alle impegnative attribuzioni conseguenti al nuovo quadro giuridico europeo (in particolare rispetto a data breach, valutazioni di impatto, sistemi di certificazione e codici di condotta europei, obbligatorietà del parere sulle norme primarie), ma anche a normative nazionali di settore (come in materia di accesso civico, banca dati del DNA e identità digitale, cyber bullismo), il Garante deve infatti continuare ad esercitare le proprie funzioni "tradizionali".

La nostra missione principale è ora quella di preparare la transizione, accompagnando, da un lato, organismi pubblici e imprese a conformarsi alle nuove regole in un quadro di certezza del diritto e, dall'altro, le persone a diventare consapevoli delle garanzie rafforzate e dei nuovi diritti riconosciuti dal Regolamento.

Così, abbiamo tracciato una prima Guida che ne illustra le principali innovazioni e fornisce indicazioni utili sulle prassi da seguire e sugli adempimenti da attuare. Lavoriamo, inoltre, intensamente insieme ai nostri omologhi a livello europeo per sviluppare linee guida comuni volte a uniformare e chiarire l'interpretazione delle disposizioni chiave della nuova disciplina.

DPO, diritto alla portabilità dei dati, valutazione d'impatto privacy e sportello unico per i trattamenti transnazionali, sono le prime importanti novità su cui abbiamo fornito raccomandazioni e chiarimenti.

Di fronte alla complessità delle questioni con cui tutti i giorni ci misuriamo (come dimostra la più dettagliata illustrazione dell'attività svolta che trovate nella Relazione) e alle sfide sempre nuove nei numerosi settori che dobbiamo presidiare, avvertiamo forte e urgente la necessità di potenziare l'Autorità, adeguandola ai nuovi compiti con un significativo incremento del personale, analogamente a quanto stanno facendo i maggiori paesi europei.

Lo prevedono espressamente le stesse disposizioni del regolamento e della Direttiva. E lo ha raccomandato all'Italia il Consiglio dell'Unione, a seguito della valutazione nel 2016 sull'applicazione, da parte del nostro Paese, dell'acquis di Schengen, per consentire all'Autorità l'effettivo esercizio dei propri poteri di controllo sulle banche dati del SIS e del VIS.

Chiediamo al Governo e al Parlamento di condividere tale imprescindibile necessità e sostenere il nostro impegno in questa direzione, prima di tutto per difendere i diritti dei cittadini.

Ma anche perché sarebbe incomprensibile se un Paese che vuole competere nell'economia fondata sui dati non dovesse investire nella protezione dei dati.

Per concludere, ringrazio il Segretario generale e tutti coloro che nell'Ufficio, ogni giorno, lavorano con generosità e competenza per mantenere alto il prestigio e l'efficienza della nostra Autorità.

E naturalmente desidero ringraziare le Colleghe che con me compongono il Collegio del Garante, con le quali persiste un solido rapporto di fiducia e collaborazione, grazie al quale è stato possibile conseguire i risultati illustrati.

I numeri del 2016

Provvedimenti collegiali 561

277
Ricorsi decisi

122
Ordinanze-ingiunzione

29
Verifiche preliminari

20
Pareri resi al Governo

9
Autorizzazioni generali per i dati sensibili e giudiziari

4.633
Riscontri a segnalazioni e reclami

€ 3.289.896
Sanzioni riscosse

282
Ispezioni

2.339
Sanzioni contestate

2.369
Notificazioni pervenute

53
Comunicazioni all'autorità giudiziaria

24.097
Risposte a quesiti

50
Comunicati e *newsletter*

5.019.947
Accessi al sito web