GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

L’universo dei dati e la libertà della persona

Discorso del Presidente

Antonello Soro

Relazione2018

Piazza Venezia, 11
00187 Roma
Tel. 06 696771
e-mail: garante@gpdp.it
www.garanteprivacy.it

Relazione2018

Discorso del Presidente

Antonello Soro

Roma, 7 maggio 2019

Signor Presidente, Autorità, Signore e Signori,

presentiamo questa Relazione in conclusione del nostro mandato.

In questi anni è profondamente mutato il contesto sociale, economico, culturale e, con esso, il senso e l'orizzonte dell'azione dell'Autorità, così come il valore e la portata del diritto affidato alla sua tutela.

Le nuove tecnologie, che hanno consentito straordinarie e irrinunciabili conquiste per l'umanità, hanno progressivamente trasferito nello spazio digitale una parte significativa delle attività private e pubbliche.

I dati, proiezione della persona in questa nuova dimensione della vita, alimentano lo sviluppo in ogni campo delle scienze e costituiscono il fondamento della nuova economia.

Il digitale è divenuto agente potentissimo di trasformazione sociale, struttura e sovrastruttura insieme: la cornice entro cui si dispiegano libertà e responsabilità, spingendo l'uomo a trascendere i suoi stessi limiti.

E con l'ambiguità di ogni tecnica, ma anche con la forza propria delle rivoluzioni epocali, il digitale può essere presupposto tanto di espansione quanto di limitazione delle libertà, se si inverte il rapporto tra mezzo e fine.

Governarne l'innovazione in funzione della tutela della persona e delle libertà è, allora, il vero obiettivo, da cui dipendono presente e futuro delle nostre società, con implicazioni che si estendono a ogni campo della vita individuale e collettiva. Dal lavoro alla salute e alla ricerca scientifica, ma anche alla giustizia, che in alcuni Paesi sta già avviandosi a divenire "predittiva", affidando agli algoritmi persino quelle decisioni dirimenti sull'uomo (colpevolezza, libertà, punibilità), che sembravano l'ultimo baluardo del dominio della razionalità umana.

Le tecnologie digitali intervengono nella definizione di criteri valoriali, orientando sempre più le decisioni sia individuali che collettive e, per altro verso, concorrono a delineare l'esercizio della sovranità, modificando equilibri geopolitici prima indiscussi.

Lo stesso antagonismo commerciale tra USA e Cina sottende una competizione per l'egemonia tecnologica, che disegna la nuova geografia del potere planetario.

Il possesso e lo sfruttamento dei dati, che si accumulano nell'infosfera, sono la posta in palio.

A confronto sono due potenze che hanno maturato le proprie posizioni di vantaggio competitivo sulla raccolta massiva di dati, resa possibile da norme poco attente alle implicazioni di tale forma di "accumulazione estrattiva" sulle libertà individuali.

Tuttavia, se negli USA si sta avviando un percorso di rafforzamento della privacy, a seguito della sentenza Schrems e delle rivelazioni su Cambridge Analytica - che hanno dimostrato come la protezione dei dati sia un presupposto indispensabile di autonomia e sovranità - la realtà cinese sembra muoversi in senso assai diverso.

E l'entità dei rapporti commerciali tra Europa e Cina è tale da non poter più prescindere da una cornice di garanzie adeguate, soprattutto per la tutela dei dati, all'esito di auspicabili riforme quali quelle che hanno consentito la conclusione del Privacy Shield con gli USA e del recente accordo con il Giappone.

La sinergia tra assenza di norme efficaci a tutela della privacy e dirigismo (anche) economico favorisce, infatti, una sostanziale osmosi informativa tra i provider e il Governo cinese che, anche per ragioni culturali, può massivamente raccogliere dati personali, da riutilizzare per le finalità più diverse: dalla sicurezza nazionale alla promozione dell'intelligenza artificiale.

E persino per la realizzazione di un sistema di controllo sociale fondato sul capillare monitoraggio e la penalizzazione di comportamenti ritenuti socialmente

indesiderabili, con la preclusione all'accesso persino a determinate scuole o ad altri servizi di welfare.

La "vita a punti" dei cinesi sembra così indicare il rischio di un nuovo totalitarismo digitale, fondato sull'uso della tecnologia per un controllo ubiquitario sul cittadino e su un vero e proprio capitalismo della sorveglianza.

Sorveglianza e algocrazia

La potenza del *machine learning* ha raggiunto livelli tali da farne temere l'uso spregiudicato a fini militari, in un contesto in cui sempre più le ostilità tra gli Stati si dispiegano nella realtà cibernetica.

I microchip cognitivi, applicati al comparto della Difesa, potrebbero mutare radicalmente, nell'incertezza del diritto internazionale, il futuro campo di battaglia, con la disponibilità di sistemi mobili robotizzati in grado di emulare la percezione e i processi decisionali dell'uomo.

Per altro verso, vengono progettati algoritmi per valutare tanto l'idoneità allo sviluppo dell'embrione da impiantare in utero, quanto la prognosi di sopravvivenza dei pazienti ricoverati.

La vita e la morte - i temi ultimi su cui ancora residuava mistero - divengono, così, oggetto anch'esse di valutazioni predittive affidate ad algoritmi che, se non esenti da pregiudizi (di genere, etnia, ceto) rischiano di replicare, in progressione geometrica, le discriminazioni da cui avevano promesso di liberarci.

Le esperienze di questi ultimi anni rendono sempre più urgente affrontare il tema della democrazia nella società digitale e gli effetti distorsivi dello slittamento, della profilazione e del *nudging*, dal piano commerciale a quello politico.

Significativa, in tal senso, la vicenda Facebook-Cambridge Analytica, oggetto di un nostro provvedimento inibitorio ed alla base della recente norma dell'Unione, che sanziona l'uso illecito di dati personali per condizionare i risultati elettorali.

La prospettiva è aggravata dalla concentrazione di tali informazioni (e del conseguente potere di condizionamento) in capo a poche imprese, capaci così di spiegare effetti determinanti su questioni di rilevanza pubblica primaria.

Si destrutturano, così, presidi democratici essenziali, quali quelli volti a garantire la libera formazione del consenso elettorale e la fisiologica competizione tra partiti.

Torna, invertito, lo schema gramsciano dell'egemonia sovrastrutturale, fondata oggi sulla capacità di orientare i comportamenti con la persuasione permanente.

Sul piano sociale, ne risulta un effetto di polarizzazione estremistica dovuta alla prevalenza, accordata dall'algoritmo, a contenuti aggreganti, fondati sull'ostilità nei confronti del "nemico opportuno".

Nella società disintermediata, dalle esistenze - si è detto - "in apparenza trasparenti, ma sempre più chiuse in universi impermeabili", il 'pensiero lento', mediato dalla razionalità, risulta assai meno interessante.

Paradossalmente, quindi, il potenziale globalismo digitale rischia di promuovere, anziché capacità generativa, il riflesso autistico e antagonista delle "bolle" risultanti dai filtri e del pregiudizio conformativo, determinando un pericoloso ermetismo sociale.

Neutralità, statuto proprietario e, più in generale, sostenibilità etica e giuridica della tecnologia divengono, quindi, una questione democratica ineludibile.

Così come la sovranità si fondava, classicamente, sull'esclusività dell'uso legittimo della forza, oggi si basa sul dominio della potenza di calcolo, che non può quindi sottrarsi a una progettualità etica, politica e anche giuridica: non può, in altri termini, restare avulsa dalla forma democratica.

È questo l'obiettivo dell'Europa che, non solo con il codice etico per l'intelligenza artificiale ma soprattutto con i principi fondativi della disciplina di protezione dati, intende coniugare innovazione e dignità.

Determinante, in questo senso, il principio di trasparenza algoritmica e il diritto di contestare la decisione assunta in via automatizzata, consentendo anche l'intervento umano per sottrarre le decisioni sulle persone al totale determinismo delle macchine. Che, se da un lato possono ridurre il rischio di errori e di un uso scorretto della discrezionalità, dall'altro non possono sostituire l'attività valutativa dell'uomo, nella sua complessità, assicurando quelle garanzie di partecipazione, trasparenza e accesso, in cui si esprime la democrazia.

Del resto, se in questo campo l'Europa potrà assumere un ruolo trainante sarà non tanto e non solo per le risorse stanziate, quanto piuttosto per la leadership culturale che può promuovere, mettendo la tecnica al servizio dell'uomo, secondo il principio di responsabilità.

Questo è il contesto in cui la protezione dati ha visto mutare profondamente il proprio orizzonte di senso, sino a divenire essenziale presidio di libertà e democrazia nella complessità della società digitale.

E di fronte all'incessante progresso di una tecnologia che sembra aver smarrito il valore del limite, questa disciplina rappresenta un efficace strumento di tutela non solo dell'identità ma anche della dignità dell'uomo rispetto al potere della tecnica, per impedire la riduzione della persona a cosa, la monetizzazione della libertà: un fattore di riequilibrio delle asimmetrie che caratterizzano i rapporti tra i cittadini e i detentori del potere pubblico e privato.

Il prezzo della libertà

Il diritto alla protezione dei dati personali viene sempre più invocato di fronte alle innumerevoli "servitù volontarie" cui rischiamo di consegnare noi stessi, in cambio di utilità e servizi che paghiamo al prezzo di porzioni piccole o grandi della nostra libertà.

Emerge così un nuovo sottoproletariato del digitale, un "Quinto Stato" formato da quanti siano disposti a cedere, con i propri dati, la libertà, in cambio dei servizi offerti in rete solo apparentemente 'a prezzo zero'.

Si muove in questa ambiguità la proposta di attribuire un "dividendo dei dati" agli utenti della rete, per consentire loro di beneficiare almeno in parte della ricchezza prodotta, con i propri dati, dai big tech. E, pur mirando a riequilibrare rapporti - quali quelli tra utenti e titolari delle piattaforme - caratterizzati da un'incolmabile asimmetria, anche questa proposta non si emancipa dall'idea della monetizzazione dei dati personali, che rappresenta oggi un tema ineludibile per le democrazie.

Non più la merce ma il dato incorpora, infatti, una relazione tra persone e assume il ruolo tradizionalmente svolto da capitale e lavoro, nella sua duplice veste, tuttavia, di risorsa economica e di oggetto di un diritto fondamentale**.**

Di qui anche la funzione pro-concorrenziale della privacy: si pensi al diritto alla portabilità che, soprattutto se accompagnato dall'interoperabilità dei sistemi, potrebbe contrastare i fenomeni anticompetitivi del *lock-in*.

Si pensi anche alla possibile qualificazione, come pratiche commerciali scorrette, delle informative reticenti o, come abuso di posizione dominante, di illecite concentrazioni di *data set* anche di terze parti, secondo dinamiche emerse, ad esempio, nel provvedimento sul caso Facebook-Whatsapp.

Gli obblighi di correttezza e trasparenza del trattamento, imposti dalla disciplina di protezione dati, possono in questo senso rappresentare una risposta determinante ai principali fallimenti del mercato digitale, superando lo schermo della territorialità, grazie alla prevista applicazione del Regolamento a chiunque offra beni, servizi o monitori il comportamento di quanti si trovino in Europa.

In questo senso, la protezione dati può rappresentare un requisito di tutela del consumatore e "*antitrust by design*" in quanto consente il governo dell'elemento fondativo dell' "economia del prezzo-zero": il dato personale.

Regolarne le condizioni di utilizzo, l'ambito di circolazione, le garanzie per l'identità che riflette, significa dunque armonizzare economia e persona, tecnologia e umanità, sicurezza e libertà.

Di qui anche la curvatura pubblicistica di questa disciplina: presidio di dignità del singolo ma anche presupposto di correttezza ed equità dell'economia "dei *like*", strumento di governo del mercato in funzione di tutela della persona.

Norme e confini

Non sarebbe democraticamente sostenibile un regime in cui i grandi gestori delle piattaforme tecnologiche, attraverso protocolli informatici o condizioni generali di contratto, stabiliscano il codice normativo su cui fondare diritti e doveri nella dimensione digitale: contesto in cui più di ogni altro si dispiega la nostra esistenza.

Da questa consapevolezza nasce il nuovo quadro giuridico, attraverso il quale l'Europa può ritrovare un ruolo di protagonista nello scenario globale, altrimenti egemonizzato dal nuovo bipolarismo sino-americano.

Con il passaggio a una disciplina di unificazione, la norma interpreta questo disegno sovranazionale e l'aspirazione universalistica al riconoscimento della protezione dati in una dimensione che supera i limiti imposti dal principio di territorialità.

Muta la stessa natura delle nostre Autorità, proiettate, ancor più nettamente rispetto al passato, in ambito europeo, ove grazie alle procedure di cooperazione e coerenza potranno rivolgersi davvero, con una voce sola, a interlocutori, come le grandi piattaforme, attratte in altri e ben diversi ordinamenti. In questa prospettiva, sarà sempre più determinante l'azione di *enforcement,* per verificare che il principio di responsabilizzazione sia interpretato davvero nel segno dell'incremento delle garanzie.

Sul piano interno, il rango del Regolamento rafforza la centralità della disciplina europea e l'efficacia della tutela multilivello dei diritti, delineando con le sue norme un limite per lo stesso legislatore nazionale.

Il parere obbligatorio del Garante sulla normativa primaria si è dimostrato, in questo primo anno di applicazione, un passaggio essenziale per delineare il miglior

equilibrio possibile tra la protezione dati e gli altri diritti e interessi di rilevanza costituzionale, nel rispetto del canone di proporzionalità, valorizzato di recente dalla stessa Consulta in relazione alla trasparenza.

Il dialogo tra Garante e legislatore ha spesso consentito apprezzabili miglioramenti dei testi, come nel caso del reddito di cittadinanza.

Maggiori resistenze si sono invece riscontrate, ad esempio, rispetto all'introduzione generalizzata dei controlli biometrici per i dipendenti pubblici.

È auspicabile che la sottovalutazione dei principi di proporzionalità e minimizzazione dei dati, riscontrata rispetto a tali provvedimenti, lasci spazio in futuro a un supplemento di riflessione, sottraendo temi così rilevanti all'enfasi della politica di parte e al conseguente rischio di norme meramente simboliche.

Ragion di Stato e Stato di diritto

Uno degli eventi più significativi del contesto in cui si è svolto il mandato di questo Collegio è stato il Datagate, che ha avuto, anche in Europa, profonde implicazioni sul rapporto tra libertà e sicurezza, protezione dati e prevenzione.

La presa di coscienza collettiva che ne è derivata ha indotto, dapprima e con più forza nelle Corti europee, la revisione della disciplina delle misure limitative della libertà per fini di sicurezza, nel segno del canone di proporzionalità.

La giurisprudenza della Corte di giustizia sulla *data retention*, giunta sino all'annullamento di un atto normativo europeo, ha in questo senso contribuito non soltanto alla generale invalidazione degli strumenti di sorveglianza massiva, ma anche al consolidamento della dimensione 'costituzionale' della protezione dati, quale parametro valutativo delle politiche pubbliche, tanto dell'Unione quanto degli Stati membri.

Sotto il profilo della *data retention* il legislatore italiano, nonostante i nostri reiterati richiami, non sembra aver colto sino in fondo le implicazioni di questi principi.

La norma - senza eguali in Europa - che consente la conservazione generalizzata e indifferenziata, per sei anni, dei dati di traffico telefonico e telematico,

costituisce una miope sfida al principio di proporzionalità ed espone il nostro Paese al rischio di censura in sede di controllo giurisdizionale di legittimità.

Tuttavia in altri campi si sono registrate innovazioni di rilievo.

Anzitutto, sul fronte dell'attività di prevenzione, proprio all'indomani del Datagate abbiamo promosso un rilevante rafforzamento del ruolo di controllo attribuito al Garante dal Codice.

Esso si è espresso attraverso nuove forme di esercizio del potere di vigilanza, disciplinate con il protocollo d'intenti siglato con il Dis nel novembre 2013 e due mesi fa ulteriormente potenziato, ma anche mediante una significativa attività consultiva che ha consentito di modulare la disciplina di settore nel segno dell'equilibrio tra prevenzione e riservatezza.

In ordine all'attività giudiziaria e, in particolare, allo strumento delle intercettazioni, sin dal 2013 abbiamo promosso l'adozione di alcune garanzie essenziali, omogenee per tutti gli uffici giudiziari, per impedire, in fase d'indagini, fughe di notizie pregiudizievoli sia di queste che della riservatezza individuale.

Dopo un'iniziale sottovalutazione del problema, si è registrato un adeguamento sostanzialmente uniforme agli standard richiesti, con beneficio non soltanto per i cittadini ma anche per la stessa attività investigativa.

Il Garante ha anche più volte, in questi anni, sollecitato Governo e Parlamento all'adozione di modifiche legislative volte a evitare il fenomeno del giornalismo di trascrizione, che si alimenta della produzione in giudizio di conversazioni irrilevanti ai fini investigativi, ma spesso gravemente lesive della riservatezza delle parti e dei terzi, coinvolti nelle indagini.

Alle iniziative assunte autonomamente da alcune Procure e poi promosse dal CSM in questa direzione, ha fatto seguito una riforma che - almeno sotto

questo profilo - tentava di limitare la trascrizione di contenuti irrilevanti, bilanciando (in maniera forse perfettibile) esigenze probatorie, diritto di difesa e privacy.

La sospensione dell'efficacia della riforma lascia sostanzialmente invariato, in tutte le sue criticità, il quadro normativo e la disomogeneità nelle garanzie derivante dalle diverse prassi adottate da ciascuna Procura, con un fenomeno di federalismo giudiziario che in tema di libertà suscita inevitabilmente preoccupazioni.

In assenza di riforme effettive, mai come in quest'ambito occorre un impegno comune.

Giustizia e informazione si caratterizzano principalmente 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. Dalla tentazione di forme comunicative che indulgano a spettacolarizzare l'azione investigativa devono essere immuni anche le forze di polizia, in un contesto in cui ogni immagine immessa in rete o sui social rischia di alimentare rancore e odio.

Per altro verso, il ricorso ai trojan a fini intercettativi - la cui disciplina non ha introdotto molte delle garanzie da noi suggerite per impedire possibili violazioni - si è rivelato estremamente pericoloso. Soprattutto nel caso di utilizzo di captatori connessi ad app e quindi posti su piattaforme accessibili a tutti, suscettibili di degenerare, anche solo per errori gestionali, in strumenti di sorveglianza massiva. Violazioni simili a quelle recentemente verificatesi vanno impedite, non potendosi tollerare errori in un campo così sensibile, perché incrocia la potestà investigativa e il potere, non meno forte, della tecnologia. Per questo, nei giorni scorsi, abbiamo segnalato al legislatore l'opportunità di una disciplina più stringente.

Alcune innovazioni positive si sono invece riscontrate rispetto alla disciplina della gestione di dati personali per fini di polizia, che a seguito delle modifiche legislative del 2015 si è articolata in una più compiuta ricognizione dei trattamenti e dei principi del Codice applicabili in materia, conferendo così maggiore certezza e organicità al quadro giuridico di riferimento.

In sede di recepimento della direttiva (UE) 2016/680, si sono poi introdotte alcune importanti garanzie ulteriori, tanto in ordine ai limiti del potere di trattamento attribuito agli organi inquirenti, quanto in ordine ai diritti riconosciuti all'interessato.

È significativa, ad esempio, la previsione del diritto della persona (a prescindere dalla posizione processuale, includendovi anche il terzo estraneo alle indagini) di richiedere, con una procedura particolarmente agile, la cancellazione o rettifica dei propri dati illegittimamente trattati in ambito giudiziario penale. Norma, questa, che potrebbe risultare particolarmente utile anche rispetto alle conversazioni intercettate.

Le tutele introdotte in sede di recepimento della direttiva si sono rivelate particolarmente preziose nella valutazione della legittimità dei nuovi sistemi d'indagine fondati, soprattutto, su *web scraping* e *social media intelligence*, ovvero sul "rastrellamento" delle fonti aperte per la raccolta di elementi utili in chiave investigativa.

Cardine di queste strategie deve essere un uso accorto della tecnologia, che non può certo offrire un vantaggio competitivo al reo rispetto agli inquirenti, solo per la difficoltà del diritto di stare al passo dell'evoluzione tecnologica. Ma che deve rispettare le libertà individuali, evitando gli eccessi deterministici della polizia predittiva, non potendo - in uno Stato di diritto - la ragion di Stato annullare le garanzie.

Identità, informazione, libertà di espressione

In ordine alla tutela dei dati personali dei minori, si è registrata dal punto di vista normativo una maggiore attenzione, espressa anche dal contributo richiesto al Garante e spesso recepito nell'ambito del procedimento legislativo.

Significativa, in tal senso, la legge sul cyberbullismo, che ha valorizzato l'esigenza di tutela in forma specifica dell'immagine e dell'identità del minore, attribuendo all'Autorità il compito di ordinare la rimozione di contenuti lesivi in caso di inerzia o rifiuto illegittimo del gestore, nei tempi celeri richiesti dalla realtà della rete.

Un equilibrio condivisibile tra tutela del minore, riservatezza e diritti dei lavoratori si era poi raggiunto, anche seguendo le nostre indicazioni, in relazione al tema della videosorveglianza negli asili per prevenire gli abusi e consentirne una più efficace ricostruzione probatoria.

La seconda lettura ha, tuttavia, alterato profondamente quest'equilibrio, introducendo misure - nella loro astratta rigidità - di dubbia compatibilità con il principio di proporzionalità.

Sul versante applicativo, invece, abbiamo avuto modo di affermare come - soprattutto ove sia in gioco la riservatezza del minore - il carattere "chiuso" del profilo di un social network non possa legittimare l'inapplicabilità delle norme di protezione dati, in ragione dell'agevole elusione dei sistemi di "chiusura" degli account e dell'intrinseca diffusività della pubblicazione in rete.

Caratteristica, questa, che deve indurre alla massima cautela nell'affidare al web i propri frammenti di vita, soprattutto se intima, di cui chiunque può appropriarsi quale strumento d'intimidazione o più in generale di coartazione della libertà, come purtroppo insegnano drammatici casi di cronaca.

Importante è stata l'evoluzione che ha caratterizzato il diritto all'oblio, riconosciuto dalla Corte di giustizia nel 2014 ma già da tempo tutelato dal Garante nella forma della deindicizzazione e valorizzato dagli istituti complementari della rettifica e dell'aggiornamento dei dati non più rispondenti alla realtà attuale.

La rettifica è stata peraltro da noi estesa allo "*snippet*" ed ha inciso anche sulla funzione di completamento automatico dei motori di ricerca, con la prescrizione della dis-associazione tra il nome dell interessato e termini pregiudizievoli, tali da ingenerare la convinzione di un suo coinvolgimento in attività illecite.

A seguito della sentenza Costeja, abbiamo delineato una specifica procedura per la tutela dell'identità nel suo progressivo costruirsi e per non cristallizzare, schiacciandola, la complessità di una biografia su un momento supe-

rato, quando non addirittura fuorviante: troppa memoria, si è detto, a volte uccide la storia.

Sul terreno della cronaca giudiziaria, attraverso la deindicizzazione si sono garantite anche - ad esempio nei casi di concessione del beneficio della non menzione della condanna nel casellario - le esigenze di reinserimento sociale del soggetto, altrimenti pregiudicato dall'essere eternamente marchiato come reo.

E la stessa giurisprudenza ha confermato come, rispetto a notizie inesatte, le tutele accordate dalla disciplina di protezione dati possano garantire, ad un tempo, la correttezza dell'informazione.

Quest'ultimo parametro, unitamente a quello dell'essenzialità, abbiamo più volte dovuto invocare, a fronte della diffusione di un eccesso di dettagli inerenti la vita privata, anche sessuale, di soggetti, persino minorenni, coinvolti in indagini giudiziarie, anche in qualità di persone offese: con il rischio di un accanimento informativo non utile ai cittadini e lesivo della dignità degli interessati, persino indulgendo al sensazionalismo o confondendo il pubblico interesse con ciò che è di interesse del pubblico.

È stato anche necessario ricordare, rispetto a un episodio di *revenge porn* in danno di un'esponente politica, il dovere del giornalista di astenersi dal diffondere dati espressivi della sfera intima individuale, privi di alcun rilievo sul ruolo e sulla vita pubblica dell'interessata.

Rispetto ad alcuni eccessi riscontrati in una nota trasmissione radiofonica, abbiamo peraltro escluso la possibilità di ricorrere ad artifici o raggiri, per raccogliere notizie acquisibili con gli strumenti propri dell'inchiesta giornalistica e di legittimare qualunque raccolta, anche illecita, di dati, in nome del solo interesse pubblico della notizia.

Non vi sarebbe, altrimenti, più alcun limite nella correttezza dell'acquisizione delle notizie e qualsiasi metodo di raccolta verrebbe giustificato in ragione del fine da perseguire.

La rilevanza assunta dalle regole deontologiche in ambito giornalistico ha indotto il legislatore a confermarne la vigenza anche nel nuovo quadro giuridico, rafforzandola peraltro con la previsione della sanzione amministrativa per i casi di violazione.

Ma al di là e prima della responsabilità in termini sanzionatori, è necessario che il giornalismo sia oggi all'altezza di un compito ben più oneroso e nobile del passato: perché lo straordinario potere di cui dispone, accresciuto dalla rete, richiede un dovere di lealtà e correttezza ancora maggiore.

Digitalizzazione e "cyberguerriglia"

La digitalizzazione dell'attività amministrativa è una componente essenziale della competitività nazionale, che va realizzata nel rispetto dei diritti dei cittadini.

In questa chiave vanno letti i nostri numerosi interventi, volti a rendere il processo d'informatizzazione - prezioso per lo sviluppo del Paese - pienamente compatibile con i principi di proporzionalità e minimizzazione, tali da circoscrivere al necessario l'espansione del patrimonio informativo pubblico, così da rendere, al contempo, esso stesso più sicuro e più efficiente l'azione amministrativa.

A fronte dell'imponente moltiplicazione e interconnessione delle banche dati pubbliche, abbiamo costantemente indicato misure per la loro razionalizzazione e messa in sicurezza.

Si pensi alle indicazioni fornite rispetto al trattamento di dati personali su larga scala che era stato previsto, dall'Agenzia delle entrate, per la fatturazione elettronica, con riguardo potenzialmente a ogni aspetto della vita quotidiana dell'intera popolazione, ritenuto sproporzionato rispetto al pur legittimo obiettivo perseguito.

Nella consapevolezza della necessità di responsabilizzare i soggetti a vario titolo coinvolti nella complessa catena della sicurezza dei sistemi e delle reti, abbiamo svolto un'importante attività ispettiva rispetto ai nodi di interscambio internet (ixp), gestiti da privati non sempre in modo adeguato e dalla cui sicurezza dipendono, tra l'altro, la sicurezza nazionale, l'efficacia delle indagini, l'incolumità dei singoli.

La parcellizzazione dei centri di responsabilità comporta, del resto, rischi cui è necessario ovviare centralizzando le competenze all'interno di una strategia unitaria, nazionale ed europea insieme, per proteggere non tanto e non solo il punto terminale ma l'"ecosistema digitale" nel suo complesso.

Altrimenti avremmo soltanto monadi protette, immerse però in un reticolo di vulnerabilità, peraltro sempre crescenti. E questo, tanto più a fronte del ricorso sempre più imponente al cloud e dello sviluppo del 5G, con cui la superficie di attacco cresce in progressione geometrica, perché i rischi si estendono a tutti i nodi della rete.

Il 2018 è stato definito, dal Clusit, l'anno peggiore relativamente alla sicurezza cibernetica, così costantemente esposta a minacce da configurare una sorta di cyber-guerriglia permanente.

E se nel settore pubblico in generale gli attacchi sono cresciuti nell'ultimo anno del 41%, in ambito sanitario l'incremento ha toccato l'acme del 99% rispetto all'anno precedente, con effetti tanto più gravi che in altri settori perché l'alterazione dei dati sanitari può determinare - come abbiamo sottolineato anche rispetto al fascicolo sanitario elettronico - errori diagnostici o terapeutici.

La carente sicurezza dei dati e dei sistemi che li ospitano può rappresentare, in altri termini, una causa di malasanità.

O, come nel caso di cui ci siamo occupati, degli embrioni scambiati, la violazione delle regole essenziali di protezione dati può avere effetti deleteri nei processi medici, tanto più gravi ove quei processi incidano su aspetti qualificanti l'esistenza individuale: la nascita, la morte, la genitorialità.

Specularmente, la protezione dei dati è un fattore determinante di efficienza sanitaria, funzionale anche alla correttezza del processo analitico fondato su big data.

Dall'esattezza dei dati utilizzati nel processo algoritmico dipende, infatti, l'"intelligenza" delle loro scelte, che tanto più in ambito diagnostico non possono tollerare errori.

La trasparenza amministrativa, tra governo del potere visibile e opacità per confusione

Innovazioni rilevanti hanno interessato la disciplina della trasparenza, con il compiuto superamento della segretezza quale forma di esercizio del potere e la mutazione del rapporto tra autorità e singolo: da autoritativo, burocratico e insindacabile a paritetico, partecipato e "controllabile"; della concezione dell'amministrazione, come servizio prima che potere; della stessa idea del cittadino, partecipe attivo della funzione di controllo democratico sull'attività pubblica.

Tuttavia, il carattere indifferenziato degli obblighi di pubblicità, unitamente all'introduzione degli accessi civico e generalizzato - che prescindono dall' interesse qualificato del richiedente - hanno reso tanto complessa, quanto necessaria, la definizione puntuale dei limiti posti alla trasparenza per esigenze di tutela della riservatezza.

Attraverso le linee guida adottate dal Garante, l'intesa su quelle dell'Anac e i numerosissimi pareri resi in materia di accesso civico, abbiamo applicato in concreto il canone di proporzionalità, su cui si misura la natura davvero democratica di questa concezione dell'amministrazione "aperta".

L'irragionevolezza dell'estensione indifferenziata dei medesimi, rilevanti obblighi di pubblicità a categorie di dipendenti pubblici del tutto eterogenee, da noi più volte rilevata, è stata del resto censurata anche dalla Corte costituzionale.

Essa ha peraltro sottolineato il rischio che l'eccesso informativo determini, con una singolare eterogenesi dei fini, opacità per confusione, ostacolando con la raccolta massiva di dati personali non tutti egualmente utili, la ricerca delle informazioni realmente rilevanti per consentire, invece, quel governo del potere visibile su cui si fonda la democrazia.

Numeri e uomini

Alla crescita del patrimonio informativo pubblico si è affiancato, parallelamente, un altrettanto rilevante aumento delle banche dati e dei sistemi di profilazione gestiti da privati.

Sono innumerevoli, infatti, le classificazioni e schedature cui ciascuno di noi è soggetto per il semplice fatto di essere o di essere stato parte di un rapporto commerciale, con la conseguente moltiplicazione esponenziale dei profili che ci riguardano.

Tanto più di fronte alla rapidissima diffusione di oggetti intelligenti - dagli elettrodomestici agli assistenti vocali fino agli *smart speaker* - che stanno entrando progressivamente nelle nostre case e i cui potenziali rischi per la riservatezza di abitudini e scelte ci sono spesso ignoti.

I nostri dati, così raccolti per i fini più vari, concorrono a ridefinire le nostre identità: quelle "transattive" derivanti dalla ricostruzione del profilo di consumatore di ciascuno e quelle "predittive" che anticipano comportamenti, scelte e persino responsabilità.

Sono, del resto, ricorrenti i tentativi - di cui ci siamo occupati - di immettere nel mercato servizi fondati su banche dati per la misurazione del *rating* reputazionale.

In gioco vi è, certamente, l'inadeguatezza di un algoritmo a svolgere valutazioni necessariamente discrezionali e complesse, quali quelle relative all'affidabilità professionale ed economica, con il rischio di errori e false attribuzioni.

Ma soprattutto vi è la sfida, culturale e antropologica, di non ridurre la complessità di una biografia al r*anking* attribuitole dall'algoritmo, sostituendo dunque i 'numeri agli uomini', per citare Federico Caffè.

Sempre più declinata al futuro nel cono d'ombra del passato, valutata per le sue propensioni desunte meccanicamente dai comportamenti pregressi, la persona finisce con il perdere il diritto al presente, schiacciata da un passato che si proietta sul futuro, assorbendo ogni altra dimensione.

All'idea della responsabilizzazione dei protagonisti del trattamento, su cui si fonda il Regolamento, si ispira poi la recente riforma della disciplina del telemar-

keting, volta a contrastare tale fenomeno, in particolare, con la prevista responsabilità solidale di titolare e responsabile, l'ambiguità dei cui ruoli ha rappresentato sinora una delle maggiori criticità.

L'efficacia di tale riforma è stata, tuttavia, depotenziata dal ritardo nell'adozione della normativa di attuazione.

Rilevante è stata anche la riforma dello Statuto dei lavoratori che, quasi cinquant'anni fa, aveva introdotto nel nostro ordinamento le prime norme a tutela della riservatezza, all'interno di un rapporto tipicamente asimmetrico quale quello di lavoro.

Tentando di adeguare norme pensate per l'organizzazione fordista del lavoro alla realtà dei sistemi satellitari e della biometria, il Jobs Act ha apportato significative innovazioni.

Con diversi provvedimenti, abbiamo cercato di offrirne puntuali interpretazioni alla luce dei principi di necessità e proporzionalità, per impedire l'abuso del potere datoriale di controllo.

La tutela accordata dalla disciplina di protezione dati, in quanto ancorata non alla forma contrattuale ma all'elemento - il dato personale, appunto - su cui si basano i controlli datoriali e la stessa gestione algoritmica del rapporto di lavoro (si pensi ai riders), diviene così un prezioso strumento di garanzia.

Significativo, in questo senso, un provvedimento nel quale abbiamo dichiarato illecita la prassi, adottata da una cooperativa, di affiggere, nella bacheca aziendale, non solo contestazioni disciplinari ma anche cartelli contenenti la valutazione professionale di ciascun dipendente, espressa mediante *emoticon.*

Una simile forma di gogna è, infatti, incompatibile con la dignità e il diritto alla riservatezza dei lavoratori.

La disciplina di protezione dati rappresenta, del resto, un presidio di tutela del lavoratore tanto più importante, quanto più le nuove tipologie di impiego

sfuggano alle forme e quindi anche alle garanzie pensate per il rapporto di lavoro tradizionale, come nel caso dello *smart work.*

Il diritto alla privacy è uno di quei diritti inviolabili protetti anche in ambito endoassociativo e per la tutela del quale siamo intervenuti, più volte, a valutare - pur nel rispetto dell'autonomia statutaria - la correttezza dei trattamenti svolti, anche riguardo all'associazionismo politico.

Oltre a prescrivere misure volte a garantire il corretto trattamento dei dati (peraltro sensibili) di iscritti ed esterni, soprattutto in relazione alla propaganda elettorale, abbiamo recentemente avuto modo di approfondire le implicazioni - illustrate anche dal Consiglio d'Europa - che la digitalizzazione degli strumenti di partecipazione politica ha sulle libertà individuali.

Da un lato, infatti, rientra nell'autonomia dell'associazione la scelta del voto elettronico quale metodo di espressione, da parte degli iscritti, della propria volontà.

Dall'altro lato, tale scelta non esime l'associazione dal rispetto dei principi essenziali di protezione dati, volti a garantire anche la libera espressione, da parte dell'iscritto, del proprio orientamento politico, al riparo da rischi di violazione, profilazione, manipolazione.

Tali garanzie sono tanto più necessarie quanto più le scelte espresse in ambito associativo si traducano poi, più o meno direttamente, in posizioni assunte dal partito o dai suoi esponenti, nelle sedi istituzionali.

Si traccia infatti, così, un *continuum* tra base, partito e luoghi della rappresentanza che, a maggior ragione, deve rispettare anzitutto le libertà fondamentali.

Un'opera collettiva

La centralità della persona è stata la "cifra" caratterizzante il mandato che a breve concluderemo, nel tentativo quotidiano di riequilibrare i rapporti tra libertà dell'uomo e determinismo della tecnica, promuovendo quella fiducia nel digitale, indispensabile per il suo sviluppo e per la sua stessa sostenibilità.

Nella progressiva affermazione universale del diritto alla protezione dati e nella sua tenuta sociale, nella sua capacità di divenire cioè forma e regola dell'agire individuale e collettivo, si giocherà una delle partite più importanti della democrazia e dello stesso ordinamento internazionale, per governare l'innovazione nel rispetto dei diritti e della dignità.

A quest'obiettivo nessuno può sentirsi estraneo: perché involge il senso stesso del nostro essere persona e la natura della società in cui viviamo.

Alla scrittura di questo fondamentale diritto di libertà dobbiamo dunque tutti partecipare, per scommettere ancora una volta tanto sulla persona quanto sul progresso.

Nel presentare la nostra prima relazione, affermavamo come, a partire dall'impostazione personalista su cui si fonda la Costituzione, sia possibile ambire a ricomporre le crescenti fratture sociali, attorno a una nuova idea di cittadinanza.

Questa è stata la nostra bussola nel percorso di questi anni, vissuti sempre con la consapevolezza del limite e, insieme, con l'ambizione di far crescere nel nostro Paese la cultura di uno straordinario diritto di libertà.

Abbiamo cercato di assolvere con tutto il nostro impegno, la nostra passione e la nostra lealtà il mandato affidatoci dal Parlamento, nel rispetto della Costituzione e con indipendenza di giudizio.

Consentitemi di ringraziare le Colleghe e il Segretario generale che hanno condiviso questa esperienza in un clima di unità e armonia, nonché i dipendenti del Garante per il loro prezioso lavoro.

Ringrazio tutte le Autorità che mi hanno onorato del loro sostegno e della loro fiducia, nonché la Guardia di Finanza per l'importante, consolidata collaborazione.

Al prossimo Collegio consegniamo un'Autorità potenziata sotto il profilo non solo delle funzioni, ma anche delle risorse umane e finanziarie.

La sfida che la attende, nel prossimo futuro, attiene all'effettività di questo diritto, che le norme hanno delineato nella massima compiutezza.

Ma la dimensione più autentica della protezione dati vive nella realizzazione quotidiana, per la quale è indispensabile il contributo di ciascuno.

Se il diritto è "un'opera collettiva", questo fondamentale diritto di libertà - che sempre più governerà il futuro nella sua complessità - lo è ancora di più.

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

stampa:
Tipolitografia Ugo Quintily S.p.A.

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

www.garanteprivacy.it