GIORNATA EUROPEA DELLA PROTEZIONE DEI DATI PERSONALI 2019

Intervento del Presidente Antonello Soro,
Presidente dell'Autorità Garante per la privacy

Nelle epoche di grande complessità e rapido cambiamento, il diritto, più di ogni altra scienza sociale, è tenuto a ridefinire lessico e semantica delineando su nuovi orizzonti la propria domanda di senso, riscrivendo categorie con la duttilità necessaria ad accogliere una realtà in costante evoluzione.
Quest'esigenza è tanto più forte in un momento, quale quello attuale, in cui le innovazioni connesse alle tecnologie digitali sembrano scardinare le coordinate del diritto: a partire dal principio di territorialità e dalla nozione di sovranità, fino alla stessa soggettività giuridica, in un contesto in cui si discute della responsabilità civile del robot.

Ogni tecnologia del resto, riflette e ad un tempo determina, con l'antropologia, anche la propria cornice giuridica: il diritto è regola non meno che definizione.
Ma nell'era digitale il rapporto di vicendevole implicazione tra tecnica, società e diritto diviene più profondo, quando superare il limite non appare più umana tracotanza - la *hybris* dell'antica Grecia - ma , come suggerisce Remo Bodei, "il maggior vanto dell'età moderna".

Viviamo in un tempo nel quale la tecnologia digitale concorre alla definizione di criteri valoriali e orienta sempre più le decisioni private e pubbliche.

E la capacità di autoapprendimento dell'intelligenza artificiale tende a marginalizzare, in molte circostanze, il contributo dell'uomo nel processo decisionale.
La rete del resto, come ogni sistema relazionale, rischia di determinare in forme nuove quelle asimmetrie - anzitutto di potere - da cui aveva promesso di liberarci e il digitale, per sua stessa natura privo di confini, diviene esso stesso confine, sempre più poroso, del nostro essere persone, segnando il limite che separa la libertà dal determinismo.

Se prive di regole, le nuove tecnologie possono alimentare un regime della sorveglianza tale da rendere l'uomo una non-persona, l'individuo da addestrare o classificare, normalizzare o escludere.

Ogniqualvolta ciò che costituisce la proiezione del sé nella dimensione digitale - il dato, appunto - viene considerato una mera cifra, da sfruttare senza considerarne

l'impatto sulla persona, essa stessa si riduce a un'astrazione priva di individualità e, dunque, di dignità.

E questo non solo per lucido calcolo di profitto o per politiche statali illiberali, ma anche solo per assuefazione alla cessione indiscriminata e disattenta, di quei frammenti di libertà che sono i dati e che incorporano sempre più relazioni tra persone e rapporti di potere.
Rileva in questo senso, soprattutto, l'intelligenza artificiale applicata alla vita individuale e collettiva, la cui progressiva diffusione ha segnato quella che – con i limiti di ogni periodizzazione – è stata definita quarta rivoluzione, con il passaggio all'internet "degli oggetti", all'economia della condivisione, al "pianeta connesso".

Internet da mezzo qual era, al pari di ogni tecnologia, è divenuto la nuova dimensione entro cui si svolge la personalità di ciascuno, la realtà in cui si esercitano e si negano i diritti, si dispiegano libertà e responsabilità.
Il tutto con straordinarie possibilità , impensabili anche solo pochi anni fa, ma anche con rischi che vanno prevenuti per porre davvero la tecnica al servizio dell'uomo, come recita il Regolamento europeo sulla protezione dati.
Significative appaiono, in questa prospettiva, le infinite innovazioni che, esemplificando, riassumiamo con l'espressione "*smart cities*":
innovazioni che assicurano un sensibile miglioramento della vita individuale e collettiva, pure al prezzo di una mappatura massiva di comportamenti e abitudini dei cittadini, secondo l'ambiguità propria di ogni tecnica, che da un lato amplifica la libertà, dall'altro la limita, se non governata in funzione di tutela della persona
Conosciamo, per il suo rilievo, l'esperienza statunitense. Sono invece meno note, ma non meno significative, altre realtà sulle quali oggi vorremmo riflettere.
Si pensi all'Estonia, che oltre a vantare città tra le più "intelligenti" ed efficienti del pianeta e ad aver introdotto da tempo diffusi sistemi di *e-voting*, ha espressamente riconosciuto l'accesso a internet come diritto fondamentale.
E tuttavia, a fronte della forte promozione delle tecnologie digitali, l'Estonia ha anche introdotto importanti limitazioni alla privacy dei cittadini.

Così Singapore, da un lato, con il progetto "*Smart Nation*" ha sperimentato droni-postino e taxi a guida autonoma, dall'altro ha legittimato, tra le deroghe ampie alla disciplina di protezione dati che pure ha introdotto, un incisivo controllo pubblico sulle persone, basato persino sul monitoraggio, con tecniche di *sentiment analysis*, dei post pubblicati sui social.

Va ancora oltre il modello cinese, caratterizzato da soluzioni avveniristiche e dall'investimento nelle tecnologie digitali delle sue grandi risorse umane e finanziarie.
Oltre un quarto delle oltre duemila compagnie di intelligenza artificiale del mondo si trovano in Cina, che in questo campo possiede una carta vincente.

La demografia, assieme all'assenza di norme efficaci a tutela della privacy, costituisce un fattore di enorme vantaggio competitivo, in un contesto economico fondato sull'intelligenza artificiale che si alimenta di quantità crescenti di dati, così come l'industria novecentesca del petrolio.

E d'altra parte la Cina compete per il primato nello sviluppo del computer quantistico e partecipa alla grande sfida per la costruzione delle maggiori reti 5G nel mondo: sfida che si intreccia a quella dell'intelligenza artificiale.
Chi costruirà le reti migliori ne dominerà i flussi, conquistando la leadership nell'intelligenza artificiale di domani.

Questa competizione, come una nuova conquista dello spazio, ha implicazioni di ordine sociale, etico e giuridico non ancora pienamente note e tali da spostare in misura significativa l'equilibrio geopolitico mondiale.
Lo stesso antagonismo commerciale tra Usa e Cina sottende una lotta per la supremazia tecnologica che ridefinisce centralità e allocazioni di potere prima indiscusse.

E' significativo che, nei giorni scorsi, a Davos sia stato proposto il tema di una governance internazionale delle tecnologie, evidenziando un generale forte interesse per una comune regolazione, ma anche la difficoltà a trovare un'architettura condivisa.

D'altra parte, in Cina, l'innesto così profondo della tecnologia nella vita privata e pubblica, si è accompagnato a una altrettanto pervasiva ingerenza dello Stato nell'esistenza individuale, in un contesto di sostanziale osmosi tra i grandi provider e il Governo, legittimato ad ottenere dai primi, per generiche ragioni di sicurezza, i dati personali di chiunque.
E' una delle peculiari espressioni del patto sociale sotteso all'attuale sistema politico cinese, fondato sulla promozione del benessere a fronte della limitazione di molti diritti civili e politici.

Le tecnologie di riconoscimento facciale sono utilizzate, sia nelle aziende che in qualsiasi spazio pubblico, come sistema di controllo sociale e prevenzione del crimine.
Pochissime informazioni sfuggono al controllo centrale o non possono essere utilizzate per affinare i modelli di *machine learning.*
E puntando sulla deterrenza dello stigma sociale, in una regione cinese si è addirittura realizzato lo schermo "della vergogna", su cui vengono proiettate le identità di indagati o di debitori insolventi.
Alcune aziende applicano sui caschi dei lavoratori sensori intelligenti per analizzare gli impulsi nervosi emessi, desumendo così lo stato emotivo del soggetto e, quindi, la sua eventuale inidoneità a svolgere certe mansioni.

In questa regressione neo-fordista, la tecnica che avrebbe dovuto liberare l'uomo dal peso e dall'alienazione della catena di montaggio rischia invece di costringerlo in nuove catene elettroniche, riducendolo a mero ingranaggio.

Ben oltre "i braccialetti" dei lavoratori, il *neuro-cap* rievoca l'orwelliana polizia del pensiero, in una postmodernità che ripropone l'uomo-automa, rappresentando una minaccia quando invece aveva promesso speranza.
Ma l'elemento forse più emblematico del sistema cinese è rappresentato dal Social Credit System, introdotto - per ora su base volontaria, dal 2020 obbligatoria - per valutare l'"affidabilità" dei cittadini, migliorare la "fiducia" nel Paese e promuovere una cultura di "sincerità" e di "credibilità giudiziaria", come annuncia lo stesso Governo, con una sorta di trasposizione sul piano sociale dei sistemi di valutazione dell'affidabilità creditizia.

Ai cittadini viene dunque assegnato un "punteggio" fondato sulla valutazione delle abitudini di acquisto, delle frequentazioni più o meno esibite, dei contenuti pubblicati in rete, penalizzando quelli socialmente o politicamente indesiderabili, con inevitabili effetti di normalizzazione.

Come una sorta di programma-fedeltà, il conseguimento di uno *scoring* alto, agevola la fruizione di servizi pubblici e privati, l'esercizio di molti diritti e libertà, mentre un punteggio basso preclude l'accesso al credito, a sistemi assicurativi o previdenziali, a determinate professioni, persino a prestazioni di welfare: una sorta di misura di prevenzione fondata non su indizi di reità ma sulla mera indesiderabilità della condotta, secondo i parametri unilateralmente decisi dal Governo.
La "vita a punti" dei cinesi è, dunque, qualcosa di più e di diverso dalla mera digitalizzazione dell'azione pubblica.
Sembra indicare la via di un nuovo totalitarismo digitale, fondato sull'uso della tecnologia per un controllo ubiquitario sul cittadino, nel nome di una malintesa idea di sicurezza.
E cambia profondamente le stesse coordinate esistenziali, riducendo la vita a valutazione permanente, svolta con insondabili logiche algoritmiche e secondo parametri assai poco trasparenti.
Questi scenari distopici sono, indubbiamente, frutto di un regime estraneo alla cultura liberale.

E tuttavia, si deve all'alleanza tra il regime e l'abuso delle nuove tecnologie **l**a realizzazione di quel panottismo digitale, descritto dal filosofo coreano Byung-Chul Han, quale sistema capillare di lettura delle parti più nascoste dell'io, tramite l'analisi dei dati disseminati da ciascuno in rete.
L'esercizio del potere diviene così, nel sorvegliato, coscienza inquieta della propria visibilità, che è essa stessa limitazione della libertà, come hanno chiarito le corti europee.

Torna dunque la tentazione e la pretesa, ad un tempo, di espropriazione di quella sfera essenziale di diritti e libertà, della stessa autodeterminazione individuale, la cui affermazione di inviolabilità, rispetto al potere statuale, si deve proprio al diritto alla privacy.
Un diritto sancito a livello internazionale, nella forma dell'immunità da interferenze arbitrarie nella vita privata, nell'immediato secondo dopoguerra, come reazione alle profonde ingerenze nelle "vite degli altri" realizzate dai regimi totalitari.
Eppure, circa mezzo secolo dopo le più importanti codificazioni internazionali dei diritti fondamentali e pure dopo l'esperienza dell'eversione interna, quei diritti di libertà affermati ieri con forza, vacillano sotto l'onda d'urto delle più varie minacce alla nostra sicurezza.
A partire da un terrorismo pulviscolare, immanente, acefalo, che elegge a bersaglio non i simboli del "cuore dello Stato" ma chiunque, rendendone così imprevedibile l'azione e del tutto casuali le vittime potenziali.
Di qui l'esigenza di un'azione preventiva a largo raggio, che si avvalga anche della 'potenza geometrica' della tecnologia in funzione antagonistica all'uso che ne fanno i "nemici" della democrazia".
Proprio in ordinamenti nati sull'affermazione dello Stato di diritto contro il totalitarismo si è tentato di introdurre limitazioni incisive, per esigenze di contrasto del terrorismo, che ne hanno messo in discussione la stessa identità.
I cedimenti talora mostrati da alcuni Stati europei sono stati sostanzialmente arginati dalle Corti, contribuendo così a ristabilire l'equilibrio tra libertà e sicurezza.
Ma proprio la diversità tra Europa e Usa nella reazione al terrorismo dimostra quanto sia stretto il nesso tra protezione dati e democrazia e quanto una sottovalutazione della prima rischi di minare la stessa essenza della seconda, soprattutto in un contesto di progressiva traslazione della sovranità, in ogni sua componente, nello spazio cibernetico.

Così l'azione investigativa si sposta dai cavi alla rete, dalle microspie ai *trojan*; i conflitti armati divengono *cyber war*, i dispositivi informatici si prestano al *dual use*.
In un contesto di progressiva erosione del confine e della sua idea, le ostilità si manifestano in maniera più sottile, alimentate da strumenti e controlli meno percettibili e più sfuggenti alle garanzie tradizionali, perché ubiquitari.
"Da qui a 5 anni avremo un robot in ogni unità da combattimento", ha dichiarato uno dei vertici dell'esercito americano e ciò non potrà non comportare un profondo mutamento dell'etica militare ma anche la necessità di adottare nuove convenzioni, per evitare incidenti dagli effetti devastanti.

Le relazioni ostili tra gli Stati si svolgono prevalentemente in rete e sin dall'attacco informatico all'Estonia nel 2007 si è discusso se in questi casi possa invocarsi un intervento della Nato, estendendo così al digitale gli strumenti pensati per la difesa dell'equilibrio internazionale da aggressioni tradizionali.

La porta d'ingresso di questi attacchi sono proprio banche dati non sufficientemente protette, come dimostrano anche le violazioni registratesi, nei mesi scorsi, nel nostro Paese.
Solo a novembre un attacco massivo, mai avvenuto prima in Italia, ha colpito circa 3mila soggetti pubblici e privati e ha portato all'interruzione dei servizi informatici degli uffici giudiziari distrettuali dell'intero territorio nazionale

Peraltro, l'episodio verificatosi di recente in Germania rivela come persino i dati meritevoli di maggiore tutela anche a fini di sicurezza nazionale siano suscettibili- se non sufficientemente protetti - di acquisizione illecita, da parte di un hacker dilettante.
Si stima che la perdita economica imputabile al *cybercrime* possa raggiungere nel 2020 i 3000 miliardi di dollari e che gli attacchi informatici possano interessare il 74% del volume degli affari mondiali.

Quella cibernetica è dunque la frontiera su cui si sta spostando sempre più e in misura più pervasiva la dinamica delle conflittualità tra Stati e tra soggetti.

Ancora una volta, contro ogni rischio di espropriazione del diritto da parte della tecnica, è proprio questa proiezione, nella dimensione digitale, dello Stato e della sua stessa sovranità a dimostrare come la protezione dati possa divenire presupposto di sicurezza, promuovendo quella resilienza indispensabile per la difesa della democrazia nel rispetto della sua identità e con mezzi, dunque, democratici.

E in proposito possiamo affermare di aver dimostrato, nel nostro Paese, come la disciplina di protezione dati, interpretata nel rispetto del canone di proporzionalità, risulti non già ostativa ma sinergica rispetto alla tutela della sicurezza nazionale.
Tale circolarità tra protezione dati e democrazia spiega perché, proprio su questo terreno, l'Unione europea abbia inteso affermare la propria sovranità digitale, in senso assai diverso da quella rivendicata dalla Cina in chiave nazionalistico-autarchica ed egemonica: bensì per la garanzia dei diritti della persona rispetto a chiunque ne gestisca, con i suoi dati, l'identità.

Affermando così non la supremazia nazionale, ma la libertà, anche oltre quei confini territoriali superati dalla rete.

Ed è significativo che, in un mondo in cui riaffiorano crescenti spinte divisive anche rispetto a questioni (clima, nucleare, dazi ecc.) sulle quali si erano consolidate posizioni comuni e condivise, la disciplina della protezione dati rappresenti, invece, sempre più un fattore di aggregazione.
Il modello europeo costituisce, infatti, non soltanto un punto di riferimento cui si stanno progressivamente ispirando un numero crescente di ordinamenti, ma anche uno dei pochissimi campi nei quali l'Unione mantiene da tempo una posizione

comune, che si sta peraltro dimostrando vincente nella governance della società digitale.

Gli stessi Usa hanno scoperto il nesso profondo che lega protezione dati e sovranità nazionale in occasione della vicenda Cambridge Analitica, essendosi accertato come molte delle comunicazioni personalizzate con inserzioni occulte, rese possibili da una disciplina della privacy troppo lacunosa, fossero riconducibili a potenze straniere, interessate a manipolare attraverso la rete il consenso elettorale.

Il condizionamento dei processi politici, da parte delle potenze straniere, mediante disinformazione e propaganda mirata in rete è stato vissuto come una "guerra mondiale dell'informazione" con una corsa agli armamenti che vede arsenali in continua evoluzione.

E se, in questo caso, la protezione dati è apparsa funzionale agli interessi nazionali e alla riaffermazione di una sovranità statuale soggetta a progressiva erosione, il presente e il futuro di questo diritto si giocano su altri orizzonti.
Quelli dell'affermazione progressiva della protezione dati come diritto universalmente tutelato, per restituire alla persona quella centralità che da tempo sembra aver perso.
Questo è il ruolo più significativo che l'Europa potrà giocare in un contesto geopolitico così fortemente segnato dal potere dell'algoritmo, ridisegnando, a partire dalla protezione dei dati, i confini del tecnicamente possibile alla luce di ciò che è giuridicamente ed eticamente accettabile.
Va in questa direzione il recente impegno delle istituzioni europee per un uso etico dell'intelligenza artificiale.

Celebrando la Giornata europea della protezione dei dati personali, ci piace pensare che se il valore di questo straordinario diritto riuscirà ad affermarsi anche in ordinamenti in cui l'ideologia del controllo sembra oggi aver ridotto la persona ad un fascio di informazioni illimitatamente acquisibili, allora - in questo tempo tanto complesso quanto affascinante - potrà dirsi vinta la più importante delle sfide lanciate all'idea di libertà dalla sinergia di tecnologia e potere.