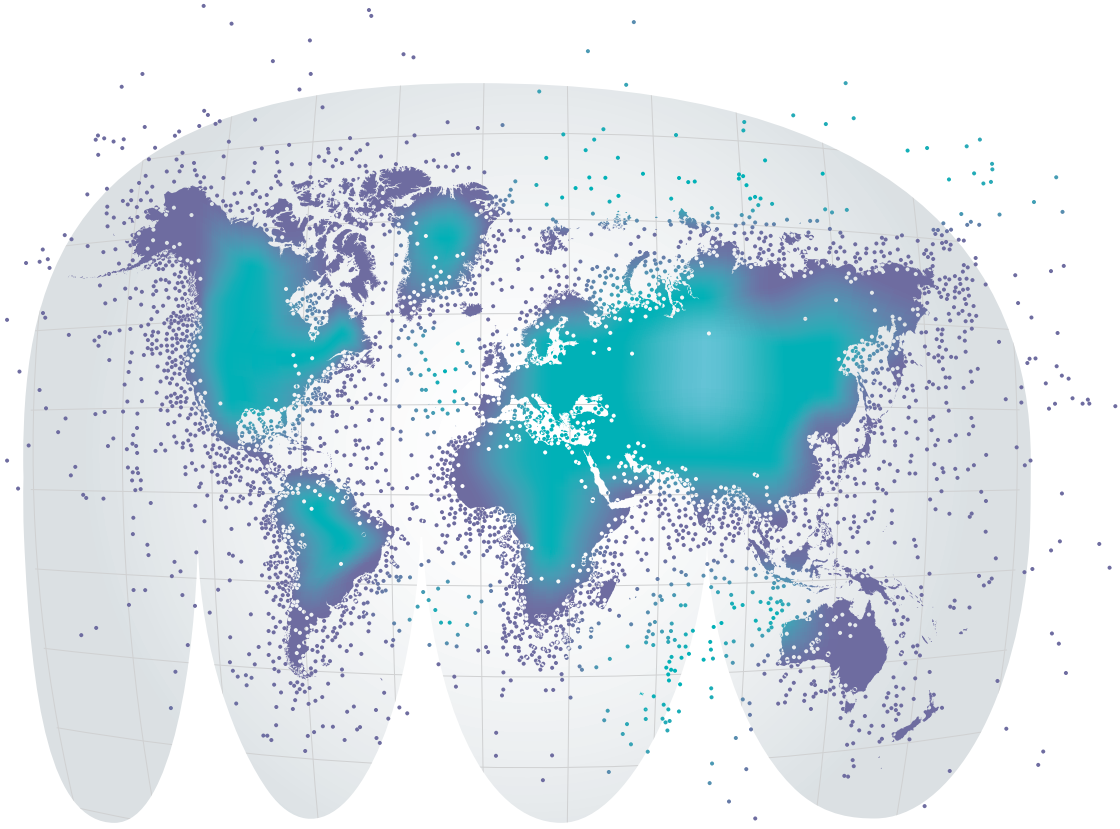
CONTRIBUTI

I Confini del Digitale

Nuovi scenari per la protezione dei dati



Atti del Convegno - 29 gennaio 2019

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Piazza Venezia, 11
00187 Roma
www.garanteprivacy.it

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

I Confini del Digitale

Nuovi scenari per la protezione dei dati

Atti del Convegno
29 gennaio 2019

www.garanteprivacy.it

In questo volume sono raccolti i contributi di studiosi ed esperti intervenuti al Convegno *"I Confini del Digitale. Nuovi scenari per la protezione dei dati"* organizzato dal Garante per la protezione dei dati personali in occasione della "Giornata europea della protezione dei dati personali" 2019.

Indice

I Confini del Digitale

Nuovi scenari per la protezione dei dati

Apertura dei lavori

Antonello Soro

Presidente del Garante

per la protezione dei dati personali

Apertura dei lavori

I Confini del Digitale Nuovi scenari per la protezione dei dati

Intervento di Antonello Soro, Presidente del Garante per la protezione dei dati personali

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 costru-

zione 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.

È 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.

È 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 la 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.

Dalle smart cities allo scoring del cittadino

Sessione I

Erica Palmerini

Docente di diritto privato dell'Istituto Dirpolis (Diritto, politica, sviluppo) della Scuola Superiore Sant'Anna di Pisa

Francesco Radicioni

Corrispondente dall'Asia per "Radio Radicale"

Coordina: **Giovanna Bianchi Clerici**

Componente del Garante per la protezione dei dati personali

Sessione I

Dalle smart cities allo scoring del cittadino

Giovanna Bianchi Clerici

È ormai considerazione comune che al macro-fenomeno della globalizzazione, corrisponda un inverso micro-fenomeno di "glocalizzazione". Di più, si potrebbe dire che questa "politica dei luoghi nei circuiti globali" eserciti una vera e propria forza centripeta attorno alle aree urbane. Una "centralizzazione" che nelle città produce un incremento esponenziale della densità demografica ed una iper-specializzazione delle funzioni pubbliche e private di offerta dei servizi al cittadino.

Le città sono i principali luoghi della produzione post-industriale: l'incubatore ideale delle *start-up* che operano nel mercato dell'*app-economy*, ben oltre il terziario avanzato. Parliamo di quella produzione di servizi virtuali di cui il giorno prima non sapevamo neppure di avere bisogno, ma quello dopo non sappiamo più come vivere senza. E benché ormai la Rete raggiunga anche gli angoli più remoti del pianeta, sono le città i nodi di questo sistema connettivo che è il digitale.

In Età Moderna, l'idea che, rispetto alla magnitudine dello Stato, con la sua imponenza e la sua forza, la città potesse costituire un modello politico è stata rifiutata ed impensabile per secoli.

Il mondo attuale, però, vede un numero sempre più considerevole di province autonome e città-regione che si gestiscono in effettiva autonomia. È un fatto come il livello amministrativo sia in via di trasferimento dagli Stati alle città, dalla dimensione nazionale a quella municipale.

Nel paragone fra centri gestionali è l'efficienza a contare e non le dimensioni dello spazio amministrato (che anzi spesso gioca a sfavore del buon governo, disperdendo sforzi e risorse).

Nell'"info-Stato" del XXI secolo, l'ultima evoluzione dei modelli socio-politici precedenti, grazie alle tecnologie dell'informazione, appunto, il settore pubblico e quello privato uniscono le forze ai fini dello sviluppo di piani strategici economici in grado di garantirne il primato.

Realtà politiche come Singapore, la City di Londra, Amburgo, Francoforte, Seoul, Zurigo, Taiwan e Milano, geograficamente molto piccole rispetto alle compagini statali tradizionali riescono a concentrare e controllare flussi di denaro, beni, risorse, tecnologia, informazione e talento, che conferisce loro un'irresistibile forza gravitazionale.

La dimensione e la geografia cittadine definiscono le *supply-chain*, sono economicamente aperte, ma allo stesso tempo riescono a risultare più protettive e difese di quanto lo possano essere quelle nazionali. Nelle limitate proporzioni di una città l'info-Stato può operare quale "tecnocrazia diretta": una post-democrazia che è in grado di combinare priorità dal basso (interpellando una popolazione numericamente ridotta e comunque concentrata) e *management* tecnocratico definito dalla capacità di dare risposte reali, piuttosto che sollevare questioni ideologiche. Le amministrazioni delle info-città o *smart cities* non perseguono una sola agenda: il loro mandato è cercare costanti miglioramenti ritagliati per la specifica e finita area di competenza (e senza poter accampare scuse, considerata la ridotta sfera d'azione ed il rapporto ravvicinato coi cittadini).

L'unica ideologia vincente è il pragmatismo.

Tutte le società desiderano ormai un equilibrio fra prosperità e vivibilità, apertura e protezione economica, *governance* efficace e ascolto dei cittadini, individualismo e coesione, libertà imprenditoriale e *welfare*. Il cittadino medio (non in senso dispregiativo) non misura tutto ciò sulla base di quanto è democratica la politica della realtà in cui vive, ma su quanto si senta sicuro nella sua città, possa

permettersi una casa ed un lavoro stabile, quali siano le sue prospettive per la vecchiaia, in altre parole quanto è in grado di rispondere alle sue necessità l'amministrazione che gestisce i suoi spazi vitali.

Tutto il resto è semplice apparenza.

La *smart city* dovrebbe, vorrebbe essere in grado di mettere a sistema tutto questo, mediante l'automazione dei processi informativi (gli *input*) e dell'elaborazione degli *output* amministrativi. La tecnologia digitale, le intelligenze artificiali in grado di leggere ed apprendere dai dati (in quantità e velocità per l'uomo impraticabili) dovrebbero consentire alla città di migliorare la vita dei suoi abitanti e visitatori in termini di rapidità ed efficientamento.

Tuttavia, se questa è la rivoluzione benefica delle *smart cities*, ne rappresenta anche il grande limite. Laddove i soli obiettivi strategici dell'azione amministrativa municipale sono pensati in termini di produttività e di eliminazione d'incidenti e tempi morti, la vita urbana si riduce all'automatizzazione delle attività e delle relazioni cittadine. L'applicazione, da parte di intelligenze artificiali programmate per efficientare, di questo pragmatismo meccanico traduce ogni rapporto in un processo da gestire ingegneristicamente e rappresenta ogni comunicazione interpersonale in termini economicistici.

È la vita stessa a finire protocollata dai sistemi di intelligenza artificiale e nei registri di *scoring* produttivo, civico, reputazionale, etc.

In uno spazio cittadino come questo, il controllo reciproco (dell'Amministrazione sui cittadini e viceversa, delle aziende fra di loro, *etc.*) si sostituisce alla fiducia, elemento fondativo per una comunità come quella cittadina. Per quanto *smart*, la città non può dimenticare la verità e la varietà del territorio, rifugiandosi nella binarietà del digitale.

L'info-città è funzionale ed efficace, ma perde quell'essenza che è nel calore assolato della piazza mediterranea, nell'ariosità dei progetti di città ideale del Rinascimento, nella passione politica dell'arengo del libero comune lombardo; quella vivacità che nasce anche dall'incontro casuale per la strada, fuori dai binari predefiniti dalla robotica.

Erica Palmerini

Tra le due formule che danno il titolo a questa prima sessione - le *smart cities*, lo *scoring* del cittadino - vi è al tempo stesso continuità e discontinuità.

Esse alludono, da diverse prospettive, a uno stesso fenomeno: quello dell'uso di massicce quantità di dati che, grazie a tecniche di *data mining* e *data analytics*, permettono di sviluppare nuova conoscenza, di gestire i servizi in modo più efficiente, di effettuare analisi predittive.

Là dove l'accento è posto sul primo termine - la *smart city* - prevale la prospettiva pubblica, della comunità. La *smart city* è al tempo stesso il soggetto gestore dei dati, che li raccoglie e li usa per far funzionare i servizi (dalla mobilità ai servizi idrici ed elettrici alla gestione dei rifiuti alla democrazia partecipativa); ma è anche la piattaforma centralizzata che li mette a disposizione dei privati perché producano innovazione. I dati raccolti dall'ambiente urbano attraverso le infrastrutture, i sensori, le apps (c.d. *user-generated data*) possono cioè essere impacchettati e rielaborati in un formato utilizzabile da sviluppatori, imprese, cittadini. Talvolta si realizza una partnership pubblico-privato, come nello scambio tra la Città di Los Angeles e la app per smartphone Waze: gli utenti di Waze rilasciano dati sull'andamento del traffico, su eventuali incidenti o avvallamenti nella strada; la città fornisce informazioni su eventi, lavori di costruzione e di manutenzione e altre iniziative che possono incidere sulla circolazione stradale[1].

Spesso le informazioni raccolte in un flusso costante, attraverso le tecnologie più varie, nel contesto delle *smart cities* non sono neppure dati personali: ad esempio, si tratta di dati ambientali (sull'inquinamento dell'aria, l'inquinamento acustico e il livello di ru-

[1] K. Finch - O. Tene, *Smart Cities: Privacy, Transparency, and Community*, in *Cambridge Handbook of Consumer Privacy*, edited by E. Selinger, J. Polonetsky, O. Tene, Cambridge, 2018, 125 ss.

more, la temperatura), il traffico di veicoli, la circolazione di pedoni e la disponibilità di parcheggi, la distribuzione geografica di certi servizi, il consumo di energia elettrica.

Quando si parla di profilazione del cittadino si accede invece alla dimensione individuale e della privacy, al tema della costruzione dell'immagine della persona attraverso tutte le tracce che dissemina nell'ambiente, reale e digitale. In questo caso, l'accento è posto soprattutto sui rischi intrinseci allo sviluppo di grandi capacità di raccolta, aggregazione e uso dei dati.

C'è insomma una visione ottimistica e per certi versi entusiastica veicolata dall'espressione "*smart city*", e invece un'aura negativa che si proietta sul fenomeno dei big data quando se ne ricava una conoscenza del singolo individuo.

La realtà è un po' più chiaroscurale. Anche nel contesto della *smart city*, l'uso dei dati può essere discriminatorio, come dimostra l'esempio di una applicazione per smartphone che, grazie all'accelerometro e alla localizzazione GPS del dispositivo, poteva essere sfruttata dalla municipalità di Boston per monitorare le buche nelle strade e intervenire più rapidamente con le riparazioni.

Ben presto ci si avvede che tale sistema avrebbe fatalmente evidenziato come bisognose di intervento le zone della città percorse da parte di persone giovani e abbienti, che più probabilmente possiedono uno smartphone, riducendo invece gli interventi nelle periferie o nelle zone più povere e finendo quindi per accrescere le disuguaglianze nel tessuto urbano. Il progetto viene così modificato per dotare della applicazione addetti incaricati di ispezionare tutte le zone, mentre i dati degli utenti sarebbero stati usati solo come informazioni addizionali[2].

Lo stigma della discriminazione colpisce anche l'ipotesi di gestire la sicurezza delle città in modalità "smart" o tecnologica.

[2] K. Finch, O. Tene, *op. cit.*, 140 s.

Notizie di tentativi controversi in questo senso talvolta provengono da oltreoceano. Ma è il quotidiano locale della città, sede della mia università, che riferisce di un progetto congiunto tra la Questura e il CNR per mettere a punto un PredPol pisano, ossia un'applicazione da installare sui display delle auto di polizia, che segnalerebbe in tempo reale le zone più esposte a rischio per piccoli crimini, sul modello di quello usato in California[3].

Per converso, la profilazione individuale, spesso guardata con sospetto, può avere ricadute vantaggiose per il singolo. ZestFinance è una compagnia che concede piccoli prestiti, a breve termine, a persone che hanno un merito creditizio modesto che li escluderebbe dall'accesso ai canali tradizionali di finanziamento. Può permettersi di farlo perché mentre le tecniche consuete analizzano una serie limitata di elementi per determinare la affidabilità del debitore, come precedenti ritardi di pagamento o episodi di insolvenza, la tecnologia a disposizione di questa impresa impiega un numero molto elevato di variabili, anche apparentemente inconferenti, che però hanno in concreto dimostrato una grande capacità predittiva.

Un secondo esempio è più ambiguo e si riferisce all'uso di certi fattori - dati estratti da carte di credito, acquisti effettuati, siti Internet visitati, quantità di ore davanti alla televisione - da parte di compagnie assicurative per identificare i clienti che sono a maggiore rischio di patologie come pressione elevata, diabete o depressione. I dati sullo stile di vita sono molto eloquenti al riguardo; e il vantaggio di questo metodo consisterebbe nella riduzione dei costi e dei tempi necessari per sottoporsi ai test sanitari. Naturalmente il sistema non appare del tutto rassicurante; inoltre, se portato all'estremo potrebbe avere l'effetto di innalzare i costi dell'assicurazione sanitaria per chiunque pratichi hobbies o abbia abitudini

[3] M. Neri, *Ecco la sicurezza 4.0: un algoritmo per prevedere rapine, furti e aggressioni*, Il Tirreno, 13 aprile 2017 <http://iltirreno.gelocal.it/pisa/cronaca/2017/04/13/news/rapine-aggressioni-e-furti-un-algoritmo-per-prevederli-1.15192360>.

alimentari non in linea con le pratiche raccomandate dai medici o, peggio ancora, di condizionare i comportamenti individuali per il timore di provocare tale conseguenza[4].

Il settore del commercio elettronico offre molte indicazioni della medesima ambiguità: l'analisi massiccia di dati attraverso algoritmi sempre più progrediti può avvantaggiare i consumatori, quando sono messi in grado di effettuare scelte più razionali perché agevolate dai siti di comparazione per un certo segmento di mercato (delle tariffe aree, alberghiere, dell'energia, delle polizze assicurative); quando possono profittare delle esperienze di altri fruitori, che le condividono attraverso le piattaforme per la recensione di molteplici servizi, e ottimizzare così le proprie scelte.

C'è il rovescio della medaglia: quando l'interazione con le imprese avviene tramite la tecnologia, ogni comportamento (dagli acquisti precedenti, ai siti visitati in varie sessioni di navigazione, al tempo di consultazione di specifiche pagine *web*, ecc.) è identificato e registrato; le proposte contrattuali possono raggiungere il consumatore in ogni momento, grazie all'ubiquità dei dispositivi digitali, ancora prima che questi abbia preso una decisione di acquisto rivolgendosi a un certo operatore commerciale; si creano i presupposti per realizzare forme di "manipolazione digitale".

Nell'ambiente digitale la conoscenza sfruttabile è infinita e l'allineamento ai bisogni e alle vulnerabilità dell'individuo può avvenire in tempo reale. Si può persino concepire un'offerta altamente personalizzata, congegnata per mezzo delle tracce che il consumatore continuamente dissemina nella rete, che detta le peggiori condizioni economiche che questi è disposto ad accettare (*price discrimination*); o che raggiunge il soggetto nel momento in cui è meno incline a resistere ad un atto di acquisto (*behavioural discrimination*).

[4] Per questi esempi v. V. Mayer-Schönberger - K. Cukier, *Big Data. The essential guide to work, life and learning in the age of insight*, London, 2013, rispettivamente a p. 48 s. e 56 s.

Eppure vi sono visioni alternative del fenomeno della *price discrimination*: secondo alcuni, benché possa avere effetti negativi sul singolo, erodendo tutto il suo potenziale di spesa, consente una massimizzazione del benessere collettivo poiché con i prezzi personalizzati si sovvenzionano i consumatori disposti a pagare meno, attraverso il surplus ottenuto da coloro che hanno una maggiore disponibilità a pagare e un maggior interesse per quel prodotto o servizio; in ultima analisi, si consente l'accesso a tale bene di più persone di quelle che si potrebbero soddisfare con prezzi uguali per tutti[5].

Con l'avvento della *Internet of things*, le opportunità per il monitoraggio delle abitudini personali cresce esponenzialmente. Si stanno diffondendo i *digital personal assistants*: nella visione dei produttori, degli *alter ego* che eseguono compiti elementari, istruiti da noi, ma che in prospettiva impareranno a conoscerci molto bene, ad anticipare ciò di cui abbiamo bisogno ed eventualmente a procurarcelo, stipulando i relativi contratti.

Sicuramente possono prestare un servizio molto utile nella riduzione della complessità delle scelte che ciascuno deve compiere quotidianamente e che prevedono una grandissima varietà di opzioni tra le quali decidere. Ma generano anche interrogativi, ad esempio sul terreno della imputazione degli effetti delle transazioni attivate da un robot: cosa succede se per errore il frigorifero intelligente ordina diverse decine di confezioni di yogurt o di un altro prodotto soggetto a scadenza, anziché la mezza dozzina che il suo proprietario è solito consumare nell'arco della settimana?

È vincolante la prenotazione che l'assistente digitale effettua presso un albergo lussuoso e molto costoso, equivocando sulle preferenze di viaggio del suo utente, anziché in quello di media categoria che avrebbe scelto per un semplice soggiorno di lavoro?

[5] Per la discussione al riguardo cfr. M. Maggiolino, *Big data e prezzi personalizzati*, in *Concorrenza e mercato*, 2016, 95 ss.

Qualche altro esempio dà un'immagine vivida degli scenari con cui dovremo confrontarci: "Hello Barbie" è la nota bambola della Mattel in cui è stato integrato un software che registra le conversazioni intorno a sé e le trasmette ad un'azienda californiana specializzata in IA, con lo scopo di migliorare la pertinenza e la qualità dell'interazione che il giocattolo ha con la sua piccola proprietaria.

La Barbie può anche fare domande e tramite le risposte acquisire informazioni sugli interessi, le attività quotidiane, la famiglia di appartenenza, molto utili per finalità di marketing [6].

Fitbit è un dispositivo indossabile che registra l'attività fisica di chi lo indossa. In almeno due casi, i dati raccolti sono stati utilizzati davanti ai giudici: per contestare una denuncia di aggressione sessuale, in cui la sedicente vittima aveva dichiarato di essere stata sorpresa addormentata, quando invece Fitbit rivelava che era sveglia e in movimento presumibilmente ad allestire la scena di violenza; in un processo civile per il risarcimento dei danni alla persona, allo scopo di dimostrare, attraverso il confronto tra il periodo precedente e successivo all'illecito, la limitazione nelle attività fisiche subita a causa dell'incidente.

Dopo queste notazioni, tra il giuridico e il sociologico, per mappare usi buoni, cattivi o dubbi della profilazione, alcune considerazioni sul quadro giuridico.

Nella discussione non municipale sulle *smart cities*, riceve molta attenzione il tema delle strategie per promuovere la protezione della privacy attraverso fonti non tradizionali: si ricorre a modelli di *soft law*, a schemi autoimposti di *privacy management*, all'implementazione della tutela della privacy per via contrattuale nei rapporti tra la parte pubblica e i numerosi soggetti, spesso privati, cui la prima appalta servizi che implicano l'uso di dati personali. L'Unione europea e, di riflesso, il nostro ordinamento sono viceversa molto avanzati sul

[6] I.D. Manta - D.S. Olson, *Hello Barbie: First They Will Monitor You, Then They Will Discriminate Against You. Perfectly*, 67 *Alabama Law Review* 2015, 135.

piano della legislazione. Occorre chiedersi, tuttavia, se questa regolazione, benché appena rinnovata, funzioni e sia adeguata alla società tecnologica e connessa.

Un primo punto problematico è la dicotomia pubblico/privato: il trattamento dei dati effettuato da soggetti pubblici è retto da un regime molto rigoroso che richiede una base normativa che lo legittimi; ciò nel solco dell'impostazione più tradizionale, risalente già agli anni '70, di assicurare protezione ai cittadini contro forme di controllo autoritario e antidemocratico. I soggetti che hanno le maggiori potenzialità di accesso ai dati personali e, altresì, le capacità economiche e le competenze per analizzarli, tuttavia, oggi sono le grandi compagnie private attive su Internet. In questo caso il principale presupposto di liceità del trattamento è il consenso dell'interessato, che si è rivelato però, secondo analisi sia teoriche che empiriche, largamente inefficace nel garantire un controllo effettivo sui propri dati personali. Da tempo è stato evidenziato come sia puramente illusoria l'immagine di un individuo che, informato delle implicazioni della propria manifestazione di volontà al trattamento dei dati, la esprime consapevolmente magari selezionando tra le alternative possibili quelle che ritiene compatibili con i propri scopi. Per la mole di informazioni che sono fatte oggetto di comunicazione, per il tecnicismo e la complessità che le connota, per i *bias* cognitivi che affliggono il consumatore e, infine, per la frequente presenza di dispositivi di semplificazione della scelta (ad esempio, la spunta di una casella che equivale ad accettazione), è stato dimostrato come il consenso non dia luogo a un reale *empowerment* del singolo[7].

[7] Cfr. European Data Protection Supervisor, *Privacy and Competitiveness in the Age of Big Data: The Interplay Between Data Protection, Competition Law and Consumer Protection in the Digital Economy* (Preliminary Opinion), marzo 2014, p. 34 s. La letteratura al riguardo è molto vasta: basti qui richiamare D. Solove, *Introduction: Privacy Self-management and The Consent Dilemma*, in 126 *Harvard Law Review* 2013, p. 1880 ss. Tra gli studi che attingono ad evidenze anche empiriche, si segnala di recente L. Gatt, R. Montanari e I.A. Caggiano, *Consenso al trattamento dei dati personali e analisi giuridico-comportamentale*, in *Nodi virtuali, legami informali: Internet alla ricerca di regole*, a cura di P. Passaglia e D. Poletti, Pisa, 2017, p. 57 ss.

Se anche un ipotetico individuo, preoccupato della propria *privacy*, leggesse le lunghe, complicate e talvolta opache informative al riguardo, non avrebbe verosimilmente nessun potere di negoziare condizioni differenti. A questo proposito, ha sollevato rilievi critici la strategia prescelta in sede di revisione della c.d. Direttiva e-*privacy*[8], che vede ancora il consenso come l'architrave sulla quale i fornitori di servizi di comunicazione digitale dovrebbero basare la propria attività. Il nuovo regolamento si applicherebbe non solo ai servizi di comunicazione tradizionale, ma anche ai servizi di messaggistica istantanea, alle telefonate tramite Internet, al calendario elettronico, agli assistenti personali digitali, alle comunicazioni *machine to machine*. In quanto disciplina speciale, in questi ambiti sarebbe destinata a prevalere sul GDPR, sottoponendo gli utenti a continue richieste di consenso - un vero e proprio "*consent bombing*" - inutile o controproducente dal punto di vista dell'autodeterminazione dell'interessato[9].

Una seconda osservazione attiene al rapporto tra tecniche di analisi dei big data e requisiti posti dal GDPR per il rispetto della privacy[10]. È stato osservato come il GDPR nasca per certi versi già obsoleto poiché non è allineato, o lo è solo marginalmente, ai nuovi processi di analisi dei dati basati su algoritmi predittivi[11].

Quali sono i principali punti di attrito?

Intanto, molti dati usati nelle analisi di big data non sono dati personali, ma è difficile isolare perfettamente le due categorie.

---

[8] Proposta di Regolamento del Parlamento europeo e del Consiglio relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/758/CE (regolamento sulla vita privata e le comunicazioni elettroniche), COM(2017) 10 final, 10.1.2017.

[9] L. Bolognini, C. Bistolfi e G. Crea, *Il Regolamento e-Privacy tra principi giuridici e impatti sull'economia digitale*, Istituto Italiano per la privacy e la valorizzazione dei dati, 2018, 15 s.

[10] I.S. Rubinstein, *Big Data: The End of Privacy or a New Beginning?*, *International Data Privacy Law*, 2013 3(2), 74 ss.

[11] A. Mantelero, *Responsabilità e rischio nel nuovo Reg. UE 2016/679*, in *Nuove leggi civ. comm.*, 2017, 145.

Dati personali e dati non personali sono concetti chiari in astratto, ma in concreto è problematico segnare un confine netto, anche per le stesse possibilità insite nelle tecniche di IA di risalire dal dato in sé non immediatamente riferibile a una persona, all'attribuzione a un soggetto determinato. La possibilità di anonimizzare i dati, così come la diversa tecnica della pseudonimizzazione prevista dal GDPR, hanno a loro volta dei limiti: oltre ai dubbi sulla fattibilità tecnica, c'è il rischio di un impoverimento dell'utilità del dato che viene reso anonimo. Ad esempio in materia di ricerca sanitaria, l'impossibilità di associare nuove informazioni ai dati esistenti riduce le opportunità di riuso dei dati, raccolti magari in ambito pubblico.

A presidiare i diritti della persona rispetto ai processi automatizzati di trattamento dei dati, compresa la profilazione, sono due previsioni essenziali del GDPR: semplificando, quella che riconosce il diritto di non essere sottoposti a una decisione basata *esclusivamente* su un processo automatizzato; e, comunque, di ottenere l'intervento del titolare del trattamento e di contestare la decisione (art. 22). La seconda consiste invece nel diritto di avere informazioni significative sulla logica utilizzata nel procedimento automatizzato (artt. 13-15). La prima norma può sembrare poco efficace, là dove si riferisce ai processi interamente automatizzati, lasciando aperta l'interpretazione secondo cui il minimo intervento da parte dell'uomo, anche solo di tipo formale, ne esclude l'applicabilità.

Del resto, neppure una revisione sostanziale darebbe garanzie sulla correttezza della decisione. Pensiamo al caso, reso noto e discusso dall'associazione ProPublica, che ha mostrato le implicazioni discriminatorie dell'impiego di un algoritmo, presso alcune corti nordamericane, per determinare il rischio di recidiva e applicare di conseguenza una pena ad esso commisurata[12]. Un'inferenza arbitraria

[12] J. Angwin et al., *Machine Bias. There's software used across the country to predict future criminals. And it's biased against blacks*, May 23, 2016, <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>.

può avere molto peso sia che il risultato prodotto dal calcolo venga applicato meccanicamente sia che il giudice, ignaro del funzionamento interno dell'algoritmo, si limiti a tenerlo in considerazione.

Quali sono infatti le chances che questi si discosti dal dato consegnato alla sua valutazione? È ovvio che il problema sta nei pregiudizi interiorizzati dal sistema, e finché questi non siano disvelati, la possibilità del controllo umano non è sufficiente a superarli.

Un altro cortocircuito riguarda il modo di funzionamento degli algoritmi applicati ai megadati e la trasparenza richiesta dal diritto ad una spiegazione della logica utilizzata. Si sostiene cioè che la trasparenza sia inutile, se non addirittura controproducente.

Gli algoritmi più efficaci sarebbero infatti quelli c.d. *black-box*, che tengono in considerazione una quantità più elevata di variabili e processano grandi moli di dati, il che li rende più affidabili nei risultati ma meno interpretabili. La necessità di fornire una descrizione obbligherebbe le imprese a scegliere algoritmi più semplici e per questo meno validi, a danno dello stesso soggetto sul quale la decisione, ad esempio ottenere un prestito, deve ricadere; oppure a impegnare risorse e competenze esperte per chiarire in termini comprensibili il modello decisionale. La necessità di rivedere i risultati del calcolo da parte di un essere umano vanificherebbe il senso del ricorso all'IA, ossia automatizzare i processi per renderli più rapidi, meno costosi e soprattutto più affidanti nei risultati. Gli obblighi imposti dal GDPR, insomma, si tradurrebbero in oneri per le imprese ma senza reali vantaggi per i consumatori. Rilievi critici riguardano anche altre previsioni del GDPR come il diritto alla cancellazione dei dati.

L'eliminazione di dati potrebbe alterare il funzionamento degli algoritmi, specialmente ove si cumulino richieste provenienti da soggetti che condividono le stesse caratteristiche, la cui incidenza verrebbe espunta dal modello di calcolo[13]. Oppure il principio di

[13] N. Wallace - D. Castro, *The Impact of the EU's New Data Protection Regulation on AI*, Center for Data Innovation, March 27, 2018.

minimizzazione dei dati, che si oppone alla logica stessa di funzionamento dei big data[14].

Queste considerazioni sono a prima vista persuasive, ma a ben vedere le garanzie poste dall'art. 22 sono, benché minime, irrinunciabili. Se le decisioni automatizzate probabilmente sono nella maggioranza dei casi più affidanti, perché oggettive e depurate dell'errore umano, l'esperienza ha rivelato che non sempre sono neutrali e, dunque, deve esserci la possibilità di una loro revisione.

È considerata una sfida della ricerca attuale in materia di scienza dei dati, quella di progettare algoritmi che sono in grado di dare una spiegazione del processo che ha condotto a un certo risultato.

E sempre nell'ambiente tecnologico c'è un'attenzione crescente per i possibili falsi dell'algoritmo, che vengono enfatizzati proprio allo scopo di mostrare come, innocui nel contesto di un'indagine sperimentale, possono avere un impatto inaccettabile se impiegati per assumere decisioni sulla vita delle persone.

Un ultimo appunto riguarda la capacità della normativa attuale di proteggere i diritti e le libertà fondamentali in una situazione di tecnologia ubiqua, in cui sensori dei dispositivi intelligenti, RFID, sistemi di localizzazione, telecamere possono raccogliere informazioni in ogni momento e ovunque, senza bisogno che ci si connetta a Internet. È sufficientemente flessibile la regolamentazione per accogliere questa realtà? Una tecnologia innovativa come quella dei droni è stata calata nella disciplina esistente[15]. Le telecamere posizionate sulla macchina

[14] O. Tene - J. Polonetsky, *Judged by the Tin Man: Individual Rights in the Age of Big Data*, 11 *J. on Telecomm. & High Tech. Law* 2013, 362.

[15] Cfr., la pagina informativa sul sito del Garante per la privacy italiano: www.garanteprivacy.it/droni; ma anche la *Guidance on the use of Drones* emanata dal *Data Protection Commissioner* irlandese nel dicembre 2015 e il documento dell'Information Commissioner's Office (ICO) inglese, *In the Picture: Data protection code of practice for surveillance cameras and personal information*, il quale dedica la sez. 7.3 proprio agli UAVs.

possono essere trattate quali forme di videosorveglianza, ancorché richiedano di adottare un approccio composito per adempiere agli obblighi di informativa, tenuto conto della mobilità dell'apparecchio, delle dimensioni e della distanza dalle persone osservate che possono renderlo quasi impercettibile[16]. Non meno importante è l'implementazione della *privacy by design* che sfrutta la tecnologia per attuare in forme integrate nei sistemi le prescrizioni sulla tutela dei dati.

Rimane da chiedersi, tuttavia, fino a che punto l'elasticità della normativa e l'interpretazione creativa delle autorità garanti possano coprire i numerosi scenari delle *smart cities*, in cui la raccolta di dati avviene in maniera costante, impercettibile, immersiva.

Francesco Radicioni

«Nell'applicazione della ricerca sull'Intelligenza Artificiale - ama ripetere Kai-fu Lee - i dati sono il nuovo petrolio e la Cina è come l'Arabia Saudita».

Perché sono partito da qui? Perché nella fondamentale battaglia geopolitica tra Cina e Stati Uniti per il primato sull'applicazione dell'Intelligenza Artificiale, Pechino non solo può contare su un'evidente vantaggio demografico - più di 800 milioni di utenti Internet, oltre la somma di quelli di Europa e Stati Uniti - ma anche di dati di più alta qualità rispetto alla Silicon Valley.

Proviamo a vedere perché. Innanzitutto - come è noto - l'universo di Internet e delle piattaforme social in Cina è completamente alternativo e autarchico rispetto a quello che conosciamo in Occidente. Infatti, negli ultimi dieci anni - uno dopo l'altro - Google, Facebook, Twitter, Instagram, WhatsApp e decine di altri siti sono

[16] *Article 29 Data Protection Working Party*, Opinion 01/2015 on *Privacy and Data Protection Issues relating to the Utilisation of Drones*, 01673/15/EN - WP 231, 16 giugno 2015.

stati bloccati dalle autorità di Pechino. Questo significa che oggi - in uno dei paesi più connessi al mondo - un'intera generazione di giovanissimi è andata per la prima volta su Internet utilizzando altre piattaforme: Baidu, Alibaba, Tencent, etc..

Non solo. In una manciata di anni i cosiddetti BAT sono passati dall'era delle copie a quella dell'innovazione, modellando il loro business sulla realtà cinese: forte localizzazione, adattamento alla navigazione da *mobile*, fortissimo impulso sulla R&S.

Sebbene ci sia qualcuno che continui a farlo, oggi non ha davvero più alcun senso definire l'onnipresente WeChat come il «*WhatsApp cinese*». Con oltre un miliardo di utenti, il gioiello tecnologico lanciato da Tencent all'inizio del 2011 è in realtà quanto di più simile a un «coltellino svizzero digitale». Una super-app attraverso cui posso chattare con gli amici, giocare on-line, trasferire denaro, comprare un biglietto dell'aereo o del treno, ordinare il pranzo, chiamare un taxi o chiedere una consulenza medica a domicilio. Insomma, senza mai uscire da WeChat, posso accedere a una serie di servizi che sulle nostre piattaforme sono parcellizzati in una lunga lista di app differenti: Facebook, Uber, Expedia, Paypal, Foodora.

Qualche numero? WeChat è installato su oltre l'83% degli smartphone presenti in Cina, una cifra che arriva al 92% nelle grandi città di prima fascia. Ricerche recenti indicano che oltre un terzo degli utenti di WeChat trascorre sulla app almeno quattro ore al giorno.

Quando mi sono trasferito a Pechino nell'estate del 2009 la Cina era essenzialmente una società fondata sul denaro contante: pochissimi erano i cinesi che avevano una carta di credito, assai diffuse erano le banconote false, per i piccoli esercizi commerciali era complesso installare il POS e una visita in banca si poteva trasformare in un'enorme perdita di tempo.

Grazie a una politica fatta di sconti e incentivi, in pochissimi anni la Repubblica Popolare si è anche trasformata in una società cashless: scannerizzando gli onnipresenti QR code si salda il conto

del ristorante, si trasferisce denaro P2P, si pagano le bollette, mentre capita persino di vedere mendicanti con il QR stampato sulla ciotola della questua.

Non bisogna pensare che tutto questo sia limitato alle grandi città. Alla fine del 2017, il 65% degli oltre 753 milioni di smartphone in Cina era stato autorizzato a pagamenti da mobile, lo stesso anno le transazioni attraverso le diverse piattaforme di pagamento da mobile avevano superato i 17 trillioni di dollari**.**

La cosiddetta rivoluzione O2O - dall'on-line e vita reale - ha consentito ai colossi cinesi di Internet di avere accesso a informazioni su abitudini e consumi dei propri utenti in modo molto più capillare e completo rispetto alle piattaforme con cui abbiamo maggiore familiarità.

Se - come abbiamo visto - i vantaggi, la comodità e l'efficienza offerta da queste app e da questi servizi spingono sempre più persone anche in Cina a condividere informazioni sulla propria vita, allo stesso tempo cresce tra i cittadini cinesi l'attenzione alla protezione del trattamento dei dati. A preoccupare c'è soprattutto la questione delle truffe on-line. Nel 2016 un sondaggio aveva indicato che non meno dell'84 per cento degli intervistati aveva subito una qualche forma di furto di dati. Mentre sono mancati scandali sul trattamento dei dati che hanno coinvolto i giganti di Internet della Repubblica Popolare, negli ultimi tempi le autorità di Pechino stanno facendo sforzi legislativi per promuovere regolamenti più restrittivi in grado di rispondere a queste nuove preoccupazioni della classe media urbana.

Può apparire paradossale: mentre aumenta la richiesta di strumenti giuridici contro lo sfruttamento economico dei dati personali, allo stesso tempo si allarga il sistema di sorveglianza del governo. Se la retorica e la legittimità del Partito Comunista si basa proprio sulla capacità delle autorità di Pechino di creare una «società stabile e armoniosa», la Repubblica Popolare non ha avuto difficoltà a giustificare enormi investimenti nella tecnologia del riconoscimento facciale sia a scopi commerciali che securitari.

Tempo fa le autorità della capitale avevano annunciato che «il cento per cento» del territorio di Pechino è monitorato da 46mila telecamere, mentre si stima che siano almeno 200 milioni gli apparecchi di sorveglianza disseminati per l'intero territorio della Repubblica Popolare: praticamente la realizzazione del Panopticon immaginato alla fine del '700 dal filosofo inglese Jeremy Bentham.

Da segnalare che oggi la Cina è anche uno dei paesi più attivi nell'esportazione di questo tipo di tecnologia, soprattutto in Africa, Medioriente e sud-est asiatico. Mentre proprio in questi nuovi mercati forte è la competizione tra i colossi cinesi e quelli della Silicon Valley anche rispetto ai servizi commerciali.

È stato però sulla rappresentazione del Social Credit System che si è visto lo iato maggiore tra quel che usciva sui giornali internazionali e il modo in cui quest'iniziativa veniva presentata sui social e sulla stampa di Pechino. Al netto della censura, i media della Repubblica Popolare hanno enfatizzavo i benefici per tutti quelli che vivono in una società con un alto livello di fiducia tra i cittadini, mentre - lo sappiamo - sui mezzi d'informazione internazionali a prevalere è stata la discrezione del Social Credit come la peggiore distopia orwelliana: un sistema a metà tra il Grande Fratello e una puntata di Black Mirror.

Come spesso succede, le cose sono un po' più complesse (anche se non meno inquietanti).

Innanzitutto, che cos'è il Social Credit System? Non si tratta di un singolo sistema di cosiddetta «vita a punti», bensì di un ecosistema di programmi e d'iniziative portati avanti da diversi soggetti - governo centrale, autorità locali, attori privati - che però condividono alcuni obiettivi di comuni. Innanzitutto, il principio che «se la fiducia si rompe in un luogo allora le restrizioni saranno applicate ovunque».

L'idea è semplice: condividere e aggregare i dati raccolti da diversi ministeri e dipartimenti, così da monitorare i comportamenti dei cittadini e metterli di fronte alle immediate conseguenze delle proprie azioni.

Finora più che un vero e proprio «punteggio di tre cifre», l'ossatura del Social Credit è fatta dalle black list e dalle red list: i numeri delle carte d'identità e codici identificativi di individui, aziende, ma anche dipartimenti del governo vengono inseriti all'interno di questo sistema binario che a seconda del livello di «affidabilità» espone a restrizioni o a privilegi.

Dallo scorso anno, sono milioni di cittadini cinesi che non possono prenotare un biglietto aereo o salire su un treno ad alta velocità. Il motivo? Il loro nome compare nella black list con cui Pechino colpisce coloro che hanno tentato di usare biglietti scaduti, acceso una sigaretta dove non era permesso fumare, usato apparecchi elettronici contro le indicazioni del personale di bordo. Oltre alla violazione di regole che hanno un diretto collegamento con la sicurezza dei trasporti, si può finire su queste black list anche per motivi completamente diversi: non aver pagato le tasse, esser stati condannati per una frode finanziaria o per non aver pagato una multa.

L'idea di Social Credit nasce per rispondere essenzialmente ad esigenze giuridico-economiche: in assenza di un consolidato sistema bancario e legale, le autorità di Pechino hanno iniziato a immaginare un modello - fortemente paternalistico - per promuovere la cultura della sincerità, dell'onestà e dei valori tradizionali per intervenire dove non arrivava la legge.

Fin dai primi anni 2000, decine sono i progetti-pilota lanciati anche da governi locali: alcuni di questi hanno un sistema di punteggio, altri enfatizzano soprattutto i vantaggi dell'avere un atteggiamento virtuoso. Nei piani di Pechino tutte queste iniziative dovrebbero essere armonizzate in un unico sistema nazionale entro la fine del 2020 in cui si premia sincerità e affidabilità, mentre si punisce chi si comporta male.

Accanto a tutte queste iniziative pubbliche, in questi anni anche i giganti di Internet della Repubblica Popolare hanno lanciato iniziative che si muovono a metà tra il Social Credit e programmi fedeltà.

Tra questi il più famoso è senza dubbio Sesame Credit, sviluppato da Ant Financial, il braccio finanziario di Alibaba, che grazie

all'enorme mole di dati raccolti è in grado di avere le informazioni necessarie per tracciare profili di affidabilità. L'algoritmo usato è segreto, anche se Sesame Credit ha diffuso i parametri attraverso cui valuta i propri utenti: per esempio, calcolando la puntualità con cui si pagano le bollette, alcune abitudini di acquisto - «chi gioca per dieci ore al giorno ai videogames può essere considerato pigro» - ma anche frequenti cambi di residenza fanno abbassare il punteggio. Per ora, l'adesione a questi programmi è volontaria, anche se a spingere milioni di cinesi a partecipare sono state le ricompense: dall'ottenere un prestito per acquisti on-line sulla piattaforma Alibaba a poter prenotare un hotel senza dover lasciare una cauzione, fino a facilitazioni per l'ottenimento di un visto per viaggiare all'estero.

Insomma, Pechino è riuscita a trasformare la propria ossessione per la stabilità sociale in un gioco a premi.

Minacce cibernetiche e sicurezza nazionale

Sessione II

Stefano Mele

Avvocato, Specializzato in Diritto delle tecnologie, privacy e cybersecurity

Roberto Baldoni

Vicedirettore generale del Dipartimento delle informazioni per la sicurezza (DIS) con delega alla Cyber e Presidente del Nucleo per la Sicurezza Cibernetica Nazionale

Coordina: **Augusta Iannini**

Vicepresidente del Garante per la protezione dei dati personali

Sessione II

Minacce cibernetiche e sicurezza nazionale

Augusta Iannini

Nella sua relazione introduttiva il Presidente Soro ha sottolineato la necessità che il diritto ridefinisca lessico e semantica, riscrivendo categorie con la duttilità necessaria ad accogliere una realtà in costante evoluzione. Ha poi ammonito che le nuove tecnologie, se prive di regole, possono alimentare un regime di tale sorveglianza da rendere l'uomo un individuo da addestrare o classificare.

Effettivamente, in questo universo digitale in cui ognuno di noi è immerso, consapevolmente ma più spesso inconsapevolmente, anche le minacce cibernetiche, attuate con le modalità più diverse e più invasive, sono finalizzate ad acquisire informazioni e quindi ad aggredire dati personali. Da questa banale constatazione, discende la necessità di qualche riflessione perché la questione non può essere liquidata brevettando dei "lucchetti" sempre più impenetrabili per impedire che si apra il vaso di Pandora. Si impongono invece prioritariamente le questioni sulle modalità con le quali si alimentano questi sconfinati contenitori e sulla trasparenza della loro acquisizione. Per evitare che alla violenza degli attacchi si opponga la violenza di una difesa che travolge diritti perché giustificata dalla gravità della minaccia.

L'esigenza di tutela della sicurezza cibernetica che è ormai parte predominante della sicurezza nazionale, ha legittimato misure limitative della privacy dei cittadini, ha consentito ampie estensioni dell'attività di prevenzione e - cosa più insidiosa - ha contagiato sempre di più la giurisdizione che, in taluni casi, utilizza parametri

di giudizio tipici della prevenzione e, talvolta, troppo permissivi rispetto alla diffusione di dati personali.

La potenza tecnologica e la capacità di analisi degli algoritmi, unita alle caratteristiche delle minacce cibernetiche nel campo del terrorismo o della stessa criminalità organizzata, ampliano le insicurezze e, conseguentemente, le risposte del controllo degli organi investigativi. Dunque si ripropone sempre il tema dell'equilibrio tra esigenze apparentemente contrapposte.

Benjamin Franklin, nel 1755, espresse la sua opinione sulla questione con una sintesi di rara efficacia: "chi è pronto a dar via le proprie libertà fondamentali per comprarsi briciole di temporanea sicurezza non merita né la libertà né la sicurezza". Ma era il 1755: nessuno poteva immaginare dove ci avrebbe portato la tecnologia digitale e quanti danni avrebbero cagionato all'economia ed alla società in generale le minacce tecnologiche. Nel rapporto CLUSIT 2018 si segnala che il 2017 è stato un "annus horribilis" in termini di evoluzione delle minacce cyber e dei relativi impatti: i costi generati dalle sole attività cyber criminali nel quinquennio 2011-2017 sono quintuplicati passando da poco più di 100 miliardi di dollari a oltre 500 miliardi nel 2017. Dunque da un lato l'obiettivo di soggetti istituzionali pubblici e privati di acquisire sempre più dati, profilarli, utilizzarli per le più diverse finalità, oltre ogni ragionevole limite; dall'altro la consapevolezza che queste informazioni possono essere maldestramente diffuse e, nei casi peggiori, utilizzate per strumentalizzare, disinformare, influenzare.

Allora, forse, nonostante il peso delle minacce cibernetiche e della necessità di tutelare la sicurezza nazionale, bisognerà ricorrere ad una specie di manuale di autodifesa del cittadino nel quale richiamare alla massima prudenza quando si cedono i propri dati, illustrare le regole da conoscere quando si utilizzano le tecnologie digitali, invocare non solo la responsabilizzazione dei titolari del trattamento ma anche quella degli interessati. Nessuno infatti affiderebbe una Ferrari a qualcuno che non avesse una patente ed ognuno dei "devices" che utilizziamo hanno le potenzialità di una Ferrari.

Per non parlare del futuro prossimo venturo rappresentato dall'Internet delle transazioni.

Quindi - e concludo - rispetto delle regole che limitano l'acquisizione dei dati a ciò che è necessario per le finalità perseguite dai soggetti istituzionali pubblici e privati. In particolare - e a titolo meramente esemplificativo - l'uso sconsiderato dei social media, i tempi di conservazione pressoché illimitati dei dati di traffico telefonico fissati da una legge che ha violato i paletti indicati dalla giurisdizione, l'uso di tecnologie invasive nella ricerca di acquisizione delle prove blandamente regolamentato da una giurisprudenza sempre più partecipe delle finalità di protezione sociale piuttosto che di quelle della tutela dei diritti fondamentali non consentono di raggiungere un soddisfacente equilibrio tra sicurezza e libertà e rendono ancora attuale a distanza di due secoli e mezzo la sintesi di Benjamin Franklin.

Non pretendo naturalmente che questi miei punti di vista siano condivisi dagli illustri partecipanti a questo secondo workshop.

I relatori non hanno bisogno di presentazione, ma sono orgogliosa di ricordare ai presenti alcune loro particolari attitudini.

Il professor Baldoni è Professore Ordinario di Sistemi distribuiti presso la Facoltà di ingegneria dell'Informazione dell'Università degli Studi La Sapienza dove guida - tra l'altro - il gruppo di ricerca in Sistemi Distribuiti; attualmente ricopre l'incarico di vicedirettore con delega alla sicurezza cibernetica ed è quindi il massimo esperto sia sul piano normativo che organizzativo dell'architettura nazionale cyber.

Stefano Mele è un avvocato partner di un apprezzatissimo studio legale dove ricopre l'incarico di Responsabile del Dipartimento di Diritto delle Tecnologie, Privacy, Cyber security e Intelligence. È Presidente della Commissione Sicurezza Cibernetica del Comitato Atlantico Italiano. Un giurista un po' particolare quindi e sono piuttosto curiosa di come affronterà - se lo affronterà - il tema sicurezza/protezione dati.

Stefano Mele

Con molto piacere impiego un minuto del mio tempo per ringraziare il presidente Soro per l'invito di oggi. Per me è un grandissimo onore essere qui e soprattutto trattare due temi a cui tengo particolarmente: quello della protezione dei dati personali e quello della sicurezza nazionale. Il primo, infatti, rappresenta l'amore profondo che nutro per la mia professione, mentre il secondo, quello della sicurezza nazionale, rappresenta il mio amore viscerale per la nostra amatissima Patria.

Quando si parla della relazione tra protezione dei dati personali e sicurezza nazionale sembra sempre di approfondire temi estremamente distanti tra loro, forse addirittura inconciliabili. Questa, però, è una visione molto miope del problema. Nel corso del tempo, infatti, abbiamo digitalizzato ogni informazione. Oggigiorno sono rarissime le attività personali e professionali che ciascuno di noi compie senza la mediazione di uno strumento tecnologico e senza la "presenza" di Internet. Rarissime sono anche le informazioni non digitalizzate: lo è la voce quando si parla attraverso uno *smartphone*; lo è la posizione geografica quando si utilizzano i servizi di localizzazione; lo sono le relazioni sociali, che avvengono sempre più attraverso i *social network* e i servizi di messaggistica; lo sono i gusti di ogni cittadino, cosa cerca, cosa gli piace, cosa acquista utilizzando Internet e le tecnologie. Tutta la vita è ormai digitalizzata, registrata, catalogata, profilata e ovviamente analizzata. Per di più, queste informazioni difficilmente saranno mai realmente cancellate, salvo appunto che una norma non lo richieda espressamente.

Del resto, è sotto gli occhi di tutti come l'elevata pervasività delle tecnologie e di Internet all'interno di ogni strato del nostro odierno tessuto sociale abbia completamente mutato - in un lasso di tempo molto esiguo - ogni aspetto della nostra società, dell'erogazione e gestione dei servizi, dell'accesso alle informazioni, della loro qualità e quantità, nonché dell'interazione tra questi elementi

e il cittadino. Come se ciò non bastasse, nella cosiddetta "società dell'informazione", le tecnologie e Internet sono ormai alla base anche dei sistemi complessi che assicurano la corretta esecuzione dei settori strategici ed essenziali di ogni Stato, come quelli dell'energia, delle comunicazioni, dei trasporti, del sistema finanziario e così via. Le tecnologie e Internet rappresentano, quindi, uno dei principali cardini intorno a cui ruota il benessere economico e sociale di ogni Stato, nonché il piano di appoggio e il motore della sua crescita.

È evidente, quindi, come in un simile contesto tutte le informazioni digitalizzate assumano un valore estremamente rilevante, a maggior ragione se prendiamo in considerazione anche i dati personali e se, soprattutto, decliniamo il loro valore in un'ottica di sicurezza nazionale.

Di questo indiscutibile valore se ne sono accorte da tempo le organizzazioni criminali, che attraverso Internet e le tecnologie sempre di più cercano di violare i sistemi di protezione posti a salvaguardia di queste informazioni, al fine di ottenere un tornaconto economico. Se ne sono accorti, soprattutto dal 2010 in poi, anche gli Stati, che attraverso le agenzie di *intelligence* e i cosiddetti *cyber command* (specifiche unità militari create per svolgere operazioni cibernetiche nel e attraverso il ciberspazio) hanno sempre di più investito e continueranno ad investire in questo settore per le loro attività di spionaggio e di difesa dai conflitti. Se ne sono accorte, inoltre, le organizzazioni terroristiche, che da un lato comunicano i loro messaggi di terrore in maniera sempre più mirata e "profilata", mentre dall'altro provano a compiere attacchi informatici - finora fortunatamente sempre di basso profilo - tesi alla sottrazione proprio dei dati personali di obiettivi sensibili (come politici, militari e personaggi noti). Infine, se ne sono accorti anche gli *hacktivisti*, che utilizzano il ciberspazio per portare all'attenzione del governo i loro messaggi politici, violando, oltre le norme del Codice penale, anche quelle relative alla riservatezza e alla protezione dei dati personali. In tale contesto, non deve passare sottotraccia, ad esempio,

come la "*Relazione sulla Politica dell'Informazione per la Sicurezza*", che ogni anno viene resa dal nostro Comparto Intelligence al Parlamento, già da tempo abbia messo in luce come la metà degli attacchi cibernetici complessivi registrati in Italia sia legata proprio alle attività degli *hacktivisti*. Di conseguenza, metà del valore della minaccia cibernetica in Italia appare basato sulla sottrazione e soprattutto sulla diffusione illecita di dati personali.

La normativa in materia di protezione dei dati personali si erge, allora, non soltanto a baluardo delle pratiche scorrette delle aziende nei confronti dei cittadini, ma anche come elemento della sicurezza nazionale dello Stato. D'altra parte, ripercorrendo la genesi di questo diritto, scopriremo che esso affonda le proprie radici non nel GDPR o nel Decreto legislativo n. 196 del 2003, ma nella Dichiarazione universale dei diritti dell'uomo del 1948, nella Convenzione europea dei diritti dell'uomo del 1950, così come nella Carta dei diritti fondamentali dell'Unione europea. Il diritto alla protezione dei dati personali, quindi, è connaturato ai nostri valori come uomini e cittadini europei. Di conseguenza, è un diritto che dobbiamo difendere e, trattandosi di un diritto fondamentale, dobbiamo soprattutto far in modo che questo sia sempre garantito anche agli altri.

Questa deve essere una costante anche nel caso in cui si analizzi questo diritto sotto la lente della sicurezza nazionale: le minacce alla sicurezza nazionale non si possono e non si devono mai risolvere nella generica e indiscriminata compressione o compromissione del diritto alla protezione dei dati personali dei cittadini. Anzi, dobbiamo comprendere che la sicurezza nazionale si rafforza al rafforzarsi del diritto alla protezione dei dati personali all'interno di uno Stato.

Del resto, da un'attenta e approfondita analisi del dettato del GDPR si può chiaramente trovare traccia di questa necessità. È presente negli obblighi che il titolare del trattamento deve assolvere per soddisfare i principi che sono alla base della normativa europea, nelle misure di sicurezza che vengono richieste per il trattamento dei dati personali, nella valutazione d'impatto sulla protezione dei

dati, così come, ancora, nell'esigenza di garantire sempre la soddisfazione dell'esercizio dei diritti degli interessati. Ci troviamo di fronte, allora, all'ennesima evoluzione, nel corso della sua esistenza, del diritto alla protezione dei dati personali, che ormai non è più, non può e non deve essere soltanto un diritto unicamente legato al singolo cittadino: la protezione dei dati personali oggigiorno è inevitabilmente un diritto collettivo. È un diritto che guarda a tutti e che quindi riguarda tutti. È il diritto per eccellenza alla base dell'attuale società dell'informazione, perché, se da un lato è teso a garantire un diritto individuale, dall'altro, invece, sottende alla tenuta complessiva dell'ordinamento democratico e del vivere civile della popolazione.

Peraltro, è proprio lungo questo tracciato che il diritto alla protezione dei dati personali, così come delineato dal GDPR e dal nostro Decreto legislativo n. 101 del 2018, incontra la Direttiva UE 2016/1148, meglio nota come Direttiva NIS, che ha come obiettivo quello di dettare le misure volte a creare un livello comune elevato di sicurezza delle reti e dei sistemi informativi all'interno degli Stati membri dell'Unione europea. Ciò avviene, in particolare, attraverso il dovere di adottare misure strategiche, di *governance* e tecniche che consentano di ridurre i rischi e l'impatto degli incidenti informatici, oltre che di favorire la cooperazione e la condivisione delle informazioni tra Stati membri. In quest'ottica, quindi, le principali direttrici attraverso cui si esplica l'azione della Direttiva NIS risultano essere, tra le varie, essenzialmente quelle di:

(I) promuovere la cultura della gestione del rischio e della segnalazione degli incidenti informatici tra i principali attori economici, in particolare tra gli operatori che forniscono servizi essenziali per il mantenimento di attività economiche e sociali, così come tra i fornitori di servizi digitali;

(II) migliorare le capacità nazionali in materia di sicurezza cibernetica;

(III) rafforzare la cooperazione nel settore della sicurezza cibernetica a livello nazionale e in ambito europeo.

È di tutta evidenza che costruire un sistema di protezione cibernetica nazionale ed europeo che permetta di creare un livello comune elevato di sicurezza delle reti e dei sistemi informativi all'interno di tutti gli Stati membri, così come all'interno di tutti gli operatori nazionali che erogano servizi essenziali per i cittadini e tra tutti i fornitori di servizi digitali, significhi parlare indiscutibilmente di sicurezza nazionale di ciasuno Stato e dell'intera Unione europea.

Se ciò è vero, però, è altrettanto evidente come questo sistema di protezione tuteli in maniera forte anche tutti i dati personali presenti all'interno dei sistemi informativi di ogni singolo Stato membro, nonché di ogni singolo fornitore di servizi essenziali e di servizi digitali. Questo obiettivo potrà e dovrà essere raggiunto mettendo in relazione - attraverso una costante osmosi - le misure di sicurezza adeguate che il Titolare del trattamento deve obbligatoriamente predisporre per il trattamento dei dati personali con quelle, sicuramente più ampie, necessarie per le finalità previste dalla Direttiva NIS.

GDPR e Direttiva NIS, che, peraltro, rappresentano solo il punto di partenza del lungo percorso che l'Unione europea ha disegnato nel settore della sicurezza cibernetica all'interno della sua nuova *cybersecurity strategy*, la quale racchiude già nel titolo ("*Resilienza, Deterrenza e Difesa: verso una Cibersicurezza forte per l'UE*") i principali pilastri strategici che intende col tempo perseguire.

In quest'ottica, tra i numerosissimi indirizzi operativi previsti dalla strategia, appaiono sicuramente molto interessanti l'ormai immiente estensione del mandato dell'ENISA a vera e propria agenzia per la sicurezza cibernetica dell'Unione europea e soprattutto la successiva creazione di un quadro europeo di certificazione della sicurezza cibernetica di prodotti e servizi. Occorre evidenziare fin da subito, infatti, come l'istituzione di un quadro europeo di certificazione contribuirà in maniera evidente anche al raggiungimento di quell'auspicabile dovere di diligenza del settore industriale utile ad implementare reali metodologie di "sicurezza fin dalla progettazione" di prodotti, servizi e sistemi. Una soluzione, questa, che si rileva ormai imprescindibile soprattutto in ragione dell'attuale mancanza

di un mercato europeo di prodotti e servizi specificatamente creati per far fronte alle esigenze di sicurezza cibernetica dei governi degli Stati membri. Una mancanza che si sostanzia in un indiscutibile punto di debolezza largamente sfruttato da alcuni attori statali per attività politiche, di spionaggio e di supporto a future operazioni militari. Per converso, tale quadro di certificazione, oltre ad aumentare la fiducia dei consumatori sulla sicurezza di ciò che viene acquistato e utilizzato, fornirà anche palesi vantaggi alle imprese, che per operare a livello transnazionale non saranno più costrette a seguire differenti processi di certificazione, limitando così anche i costi amministrativi e finanziari.

Se questo è il contesto in cui oggi ci muoviamo, appare evidente, dunque, come il diritto alla protezione dei dati personali non possa più essere disgiunto dalla sicurezza nazionale. Il dibattito, quindi, non deve più costruirsi sul tema del diritto alla protezione dei dati personali e sicurezza nazionale, ma deve trasformarsi in diritto alla protezione dei dati personali è sicurezza nazionale, ovvero è parte della sicurezza nazionale e ne è un suo elemento imprescindibile. Ciò, in quanto questo diritto, nell'attuale società digitalizzata, rappresenta uno degli elementi cardine su cui si fonda la libertà dei cittadini, la sicurezza delle imprese, la loro stabilità e competitività sul mercato, nonché la tenuta complessiva dell'ordinamento democratico. In una frase, ancora una volta, il diritto alla protezione dei dati personali è sicurezza nazionale.

Roberto Baldoni

Comincerò questa mia esposizione parlando di complessità, perché probabilmente quello che ci differenzia dal passato, anche solo da alcuni decenni fa, è proprio l'aumento esponenziale del livello di complessità dovuto ai salti tecnologici avvenuti negli ultimi anni, che si è riflesso in un incremento della complessità della società attuale, a volte creando evoluzioni e vulnerabilità che nemmeno il

futurologo più creativo avrebbe potuto immaginare. L'elemento tecnologico, a differenza di terra, aria, spazio e acqua, è stato ideato dall'uomo. Mentre, gli elementi cui accennavo prima sono governati da leggi deterministiche della fisica e della chimica prive di eccezioni, quello tecnologico è costellato di errori inseriti dal fattore umano, nella fase di progettazione e di implementazione della tecnologia.

Siamo noi a realizzare i microprocessori, a programmare i computer, a realizzare le app. In tutte queste operazioni inseriamo errori, diminuiti in numero nel tempo grazie al raffinarsi delle tecniche di *software engineering e sicurezza*, ma difficilmente si azzereranno poiché gli errori sono parte della natura umana.

Alcuni miei colleghi presenti in sala riconosceranno sicuramente questa foto a sinistra in figura: è l'esempio di miniaturizzazione avvenuto all'interno dell'ENIAC (il primo calcolatore riprogrammabile realizzato intorno agli anni Quaranta). Pensate il salto che si è fatto all'interno di questo dominio tecnologico in un tempo relativamente molto breve. La tecnologia ha completamente cambiato le carte in tavola in tutti i settori, perché è diventata sempre più trasversale rispetto ai vari domini verticali.

Pensiamo in senso ampio alla società: ho riportato nella foto al centro in figura l'aborigeno australiano descritto da Corrado Guz-

zanti in una famosa gag degli anni 90, quando su Internet si interrogava: "questa tecnologia ci porta la possibilità di scambiare un numero enorme di informazioni verso un aborigeno australiano in un micro secondo, ma in fondo io e te aborigeno che *se dovemo dì*?".

Guzzanti forse aveva ragione, in fondo non abbiamo bisogno di scambiare tutte queste informazioni con l'aborigeno. Tuttavia non poteva prevedere che la tecnologia avrebbe dato vita ad una serie di applicazioni - ad esempio i social network - che avrebbero cambiato profondamente la società mettendo persone con le stesse idee in una relazione progressivamente sempre più stretta, e rinchiudendole all'interno delle cosiddette *echo-chamber virtuali.* Un percorso di crescente polarizzazione del pensiero e delle idee che attraverso algoritmi pensati a scopi commerciali mette vicino persone che condividono fatti, cose, e opinioni espellendo da queste *chamber* coloro che la pensano in modo diverso. Tutto ciò ha polarizzato la nostra società in un modo che probabilmente nessuno di noi pensava potesse mai accadere.

Dopo la società, la tecnologia ha impattato pesantemente anche l'economia: si pensi all'evoluzione dei mercati telematici, alle transazioni elettroniche automatiche, ai prodotti finanziari evoluti, ai movimenti di capitale, fino alle cripto-valute e al fintech. È ormai lontano il tempo dei mercanti che andavano a trattare il costo delle merci attraverso i sette mari. La complessità indotta dalla tecnologia ha instaurato un ciclo virtuoso, l'economia e la società richiedono nuove tecnologie, quest'ultima fornisce nuove soluzioni, le soluzioni impattano sulla società e sull'economia. Tutto ciò aumenta la complessità del nostro tempo.

È un processo in continua accelerazione. Una accelerazione impetuosa che aumenterà nei prossimi anni con la progressiva penetrazione orizzontale dell'intelligenza artificiale, della robotica pervasiva e delle tecnologie di *blockchain* basate sui registri distribuiti. Questa accelerazione avrà certamente ripercussioni sulla società e sulla economia, e questo porterà ancora allo sviluppo di nuove tecnologie.

Se guardo a questo processo con l'occhio di un professore universitario, la considero una grande opportunità, ma dobbiamo tener presente che accanto ad una opportunità c'è sempre una minaccia che si nasconde. Dobbiamo costruire un Paese che sviluppa e usa le tecnologie nella consapevolezza dei rischi che queste comportano.

Per fare ciò dobbiamo costruire un sistema che sia resiliente ai cambiamenti tecnologici e ai cambiamenti della minaccia che si avvicenderanno nel tempo.

La minaccia usa questa complessità per trovare nuove vie per perseguire i propri scopi. Diventa una minaccia multiforme, articolandosi su diversi assi in funzione delle caratteristiche dell'attore che la esercita.

Conosciamo molto bene le problematiche legate al terrorismo, citate prima dal Presidente Soro, è sicuramente una minaccia incombente sulla quale l'Italia ha avuto una serie di intuizioni molto importanti che hanno ridotto il rischio attraverso il Comitato di Analisi Strategica Antiterrorismo (CASA), le attività dei settori di *intelligence* e di polizia. Negli ultimi anni abbiamo iniziato a vedere un altro tipo di minaccia: i cosiddetti "investimenti predatori". Società acquisite da attori ostili per motivi geopolitici più che per motivi commerciali, per depauperare un Paese delle sue competenze, le sue *skill*, il suo PIL.

Il cyber si è affermato da una quindicina d'anni come una nuova forma di minaccia: la possibilità di raggiungere in modo non autorizzato tante informazioni attraverso il mondo digitale - generatore di quegli errori citati all'inizio dell'intervento - che a volte si trasformano in vulnerabilità, utilizzate da attori ostili per penetrare i sistemi informatici e carpire le informazioni. Per avere un livello informativo molto inferiore rispetto a quello raggiungibile attraverso il cyberspazio, in passato si usavano delle reti di spie, che dal punto di vista dell'attore ostile, rappresentano un costo ed un rischio molto elevati rispetto alla asimmetria della minaccia cyber e alla inerente difficoltà di attribuire azioni nel cyberspazio.

Recentemente alcuni attori ostili hanno iniziato a utilizzare il meccanismo della disinformazione, ovvero la creazione di notizie verosimili o false date in pasto alle *echo-chamber* delle reti sociali per manipolare gruppi di persone polarizzandole in modo progressivo imprigionandole all'interno di specifiche *chamber* allo scopo di screditare una tesi o una posizione politica. Usata da un attore statuale, la disinformazione ha lo scopo di spostare le posizioni dell'opinione pubblica verso situazioni più estreme, allo scopo di destabilizzare un sistema democratico. Quando un sistema viene destabilizzato, l'attore statuale ha campo libero nel dispiegare le sue politiche di influenza nei settori lasciati liberi dal sistema attaccato impegnato nel ritrovare una stabilizzazione interna. La disinformazione è una minaccia molto difficile da affrontare sia da un punto di vista operativo che normativo, poiché il confine tra disinformazione e censura è molto labile.

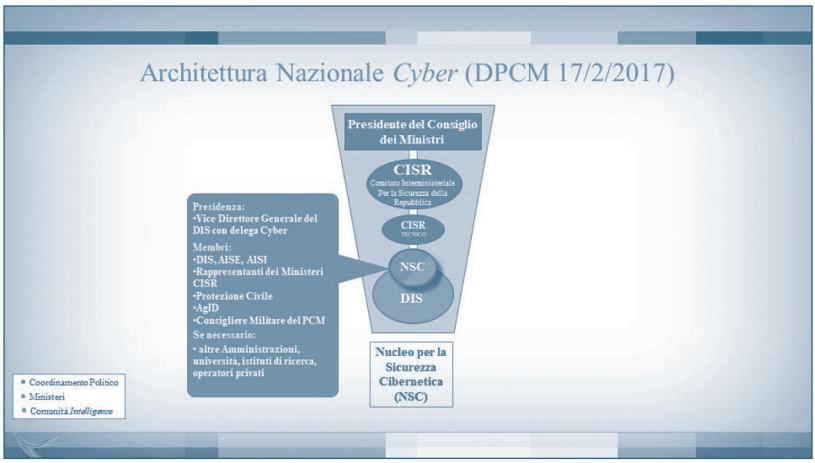
Infine pensando alle minacce del futuro, l'intelligenza artificiale è certamente in prima fila. L'intelligenza artificiale è una grande opportunità da un punto di vista commerciale, economico, di progresso, ma, cosa potrebbe accadere se venissero avvelenate le informazioni che codificano la conoscenza di una rete neurale legate alla guida autonoma? Più in generale, che cosa accade se venissero avvelenate le informazioni che utilizza un algoritmo di Intelligenza Artificiale che dovrebbe guidare verso la soluzione di un problema?

La minaccia si muove a basso livello di intensità senza superare mai dei valori di soglia predeterminati che potrebbero portare a una reazione forte da parte dell'attore attaccato, come nel caso delle soglia legata all'attivazione dell'articolo 5 della NATO. La minaccia usa, ove possibile, più elementi in modo coordinato in funzione delle caratteristiche dell'attore ostile.

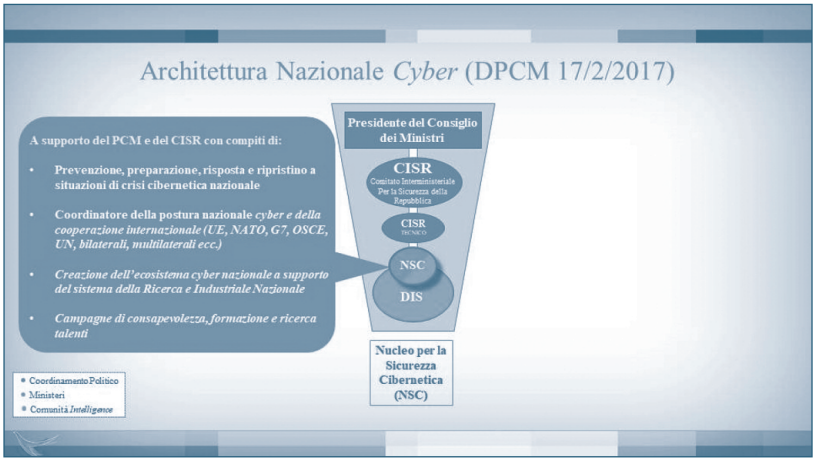
Per limitare l'impatto di queste minacce si deve lavorare su più livelli: giuridico, organizzativo e operativo. Nel settore del terrorismo abbiamo delle norme molto appropriate stratificate nel tempo. Per quanto riguarda gli investimenti predatori abbiamo approvato una legge molto importante, la così detta Golden Power, che sta dando effetti molto positivi. Nel campo della *cyber* abbiamo il DPCM di febbraio 2017, e recentemente abbiamo adottato la direttiva NIS.

Focalizziamoci ora sulla minaccia *cyber* e su come il Paese sta rispondendo. Ho parlato del DPCM del febbraio 2017, che di fatto definisce una linea di comando corta, alla cui sommità c'è il Presidente del Consiglio dei ministri, che presiede il Comitato Interministeriale Sicurezza della Repubblica, e, dal punto di vista operativo la struttura apicale è il Nucleo Sicurezza Cibernetica (NSC) alla quale afferiscono i ministeri CISR, le agenzie di intelligence, AGID, la Protezione Civile e il Consigliere Militare del Presidente del Consiglio dei Ministri. L'NSC è supportato nel suo lavoro da una organizzazione operativa interna Dipartimento informazioni per la sicurezza.

L'NSC coordina in modo rafforzato, come recita il DPCM 2/2017, i centri operativi più importanti che abbiamo in Italia: CSIRT, le strutture *cyber* di AISI e AISE, al Centro di Valutazione e Certificazione Nazionale (CVCN), che verrà presto costituito all'interno del MISE, al Comando Interforze Operazioni Cibernetiche (CIOC), alla Polizia Postale per quanto riguarda il Ministero dell'Interno. Quindi NSC può essere visto come un punto di fusione ideale per capire se un attacco informatico potrebbe essere una potenziale minaccia alla sicurezza nazionale.



Quali sono gli obiettivi dell'NSC? Innanzitutto la prevenzione, la preparazione della risposta e il ripristino a situazioni di crisi cibernetica nazionali. Il Presidente Soro ha ricordato l'incidente delle PEC avvenuto a novembre 2018: in quella occasione si è innescato il meccanismo che ha portato l'NSC alla gestione della crisi.



L'NSC lavora per cercare di creare un Paese sempre più resiliente a questo tipo di attacchi, che saranno purtroppo endemici.

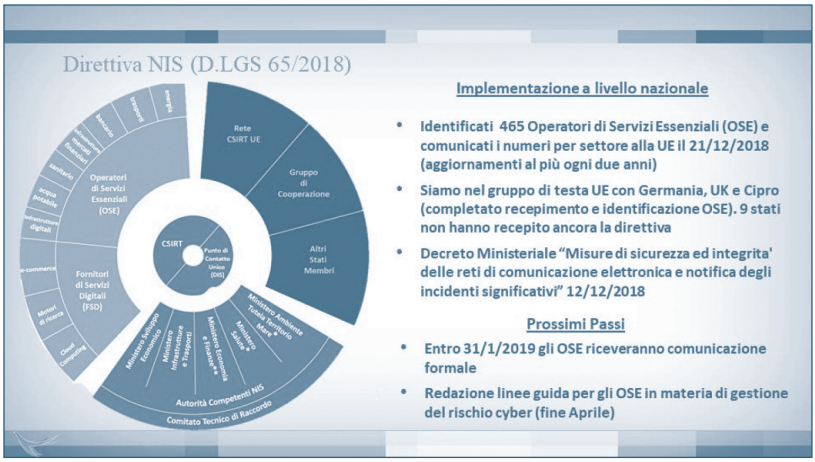
Come lo spam negli anni novanta è diventato qualcosa di endemico per i sistemi di posta elettronica, gli attacchi cibernetici lo saranno per quanto riguarda le applicazioni dell'Internet del futuro. Dobbiamo usare tutti i mezzi tecnologici, organizzativi, normativi per poter diventare un Paese resiliente a questa minaccia.

Il secondo obiettivo dell'NSC è la gestione della postura nazionale all'interno dei contesti internazionali e, come voi sicuramente sapete, poiché la minaccia orizzontale prende tutti i settori, dal sanitario all'agroalimentare al logistico, questo obiettivo diventa particolarmente arduo poiché i tavoli si moltiplicano.

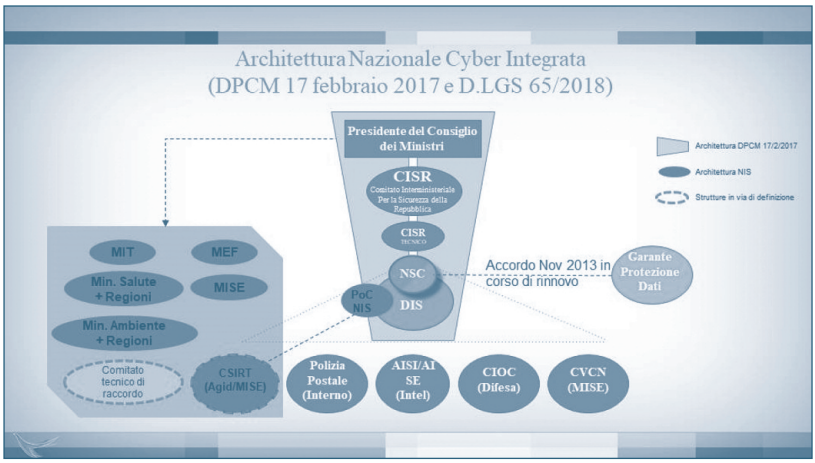
Tuttavia un grande Paese mantiene la propria barra diritta verso i propri obiettivi strategici e questo passa per una gestione coerente della postura nazionale.

Un terzo obiettivo consiste nella creazione di un ecosistema nazionale *cyber*: ricerca, industria, settore pubblico. Questo perché vogliamo cercare di sviluppare un'economia della *cyber security*, dove un buon approvvigionamento di beni e servizi arrivi da aziende del nostro Paese. Su questo siamo fortemente impegnati con le università, e le industrie nazionali. Ad esempio, la conferenza ITASEC, organizzata dal Consorzio Interuniversitario Nazionale Informatica e fortemente sostenuta dal comparto, che quest'anno ha visto oltre 1000 persone a Pisa rappresenta uno di questi momenti di formazione e consolidamento dell'ecosistema.

Infine NSC sollecita e supporta campagne di *awareness*, di ricerca talenti, e di creazione di *workforce*. Su questo spendo due parole sul programma di ricerca di talenti "*cyberchallenge.IT*" nato presso l'Università La Sapienza di Roma orientato a ragazzi dai 16 ai 21 anni. Nella prima edizione avevamo avuto 800 domande di iscrizione per 20 posti, quest'anno abbiamo avuto 3000 domande per selezionare 320 ragazzi che parteciperanno a uno dei corsi organizzati dalle 16 Università sparse sul territorio nazionale che hanno aderito all'iniziativa. Un successo che mostra anche la qualità dell'elemento umano che siamo in grado di produrre in questo Paese.



Uno dei punti importanti del lavoro del NSC è stata la direttiva NIS, attualmente in fase di implementazione. È stata promulgata a giugno 2018 e ha visto nei giorni scorsi l'identificazione di 465 operatori di servizi essenziali (OSE), i quali dovranno assicurare una gestione del rischio *cyber* ai loro sistemi allo stato dell'arte, all'interno di linee guida che verranno definite più o meno intorno alla fine di aprile dalle autorità NIS di settore. Una serie di gruppi di lavoro di settore permetteranno di elaborare delle linee guida non coercitive rispetto alle aziende. Queste ultime stanno sempre più percependo l'importanza della sicurezza come fattore di reputazione aziendale. Mentre vent'anni fa le aziende percepivano la sicurezza come un costo, oggi le aziende vedono la cybersicurezza come un fattore di qualità aziendale, e questo facilita il nostro lavoro. Infine oltre alla NIS mi piace ricordare che l'architettura nazionale cyber alla fine del 2018 si è arricchita di un altro elemento. Il cosidetto "decreto telco" emesso dal Ministero dello Sviluppo Economico nel dicembre del 2018 e che permetterà di avere notifiche di incidenti obbligatorie e controlli di sicurezza simil-NIS agli operatori di telecomunicazioni. Un provvedimento atteso da troppi anni che finalmente ha visto la luce grazie al lavoro di spinta continuo dell'NSC e alla sensibilità mostrata dei vertici di quel Ministero.



A questo punto abbiamo una architettura nazionale più articolata, mostrata in figura, dove viene mantenuta la centralità dell'NSC, perché, oltre al DPCM 17/2/2017, abbiamo il DIS coinvolto, all'interno dell'adozione della NIS, come punto di contatto rispetto alle articolazioni europee.

L'architettura nazionale *cyber* sarà perennemente in evoluzione e il suo efficace funzionamento rappresenta ora e nel futuro un bene comune, un elemento caratterizzante per la prosperità economica del nostro Paese. In questa evoluzione è particolarmente importante il rapporto con il Garante, e vorrei proprio sottolineare il passaggio fatto dal Presidente Soro sulla sinergia che occorre continuamente fare tra Garante per la Protezione dei Dati Personali e il sistema di sicurezza nazionale *cyber*. Siamo due elementi contigui. Nel contesto di questa sinergia, verrà firmato a breve un accordo che definisce uno scambio informativo rafforzato rispetto all'accordo siglato tra le parti nel 2013. Questo porterà a un flusso di eventi, che risultano avere caratteristiche di minaccia alla sicurezza nazionale, dal Garante verso NSC per essere valutati in un contesto che ha una visibilità diversa rispetto a quella più verticale del Garante.

Tra gli altri aspetti di collaborazione tra DIS e il Garante, uno per me riveste un ruolo particolare. Insieme al Centro di Ricerca di Cyber Intelligence e Information Security dell'Università degli Studi di Roma La Sapienza e al Laboratorio nazionale di *cyber security* abbiamo portato avanti una integrazione tra il *framework* nazionale di *cyber security* del 2016 e la GDPR. Questo *framework* integrato avrà un ruolo importante anche nell'applicazione della NIS ed in particolare come lingua comune da utilizzare, ad esempio, per la descrizione dei requisiti di sicurezza, che dovranno essere rispettati dagli OSE, in un contesto fortemente intersettoriale che rende complessa una applicazione omogenea della NIS sui diversi settori. Il 12 febbraio 2019, all'interno della Conferenza ITASEC di Pisa, sarà presentato il nuovo *framework* che permetterà alle aziende di avere un quadro unico tra *cyber* e GDPR come due contesti in qualche modo unificati, e fare in modo che persone, che magari lavorano in ambiti diversi dell'azienda, possano ragionare sulla stessa base di conoscenza.

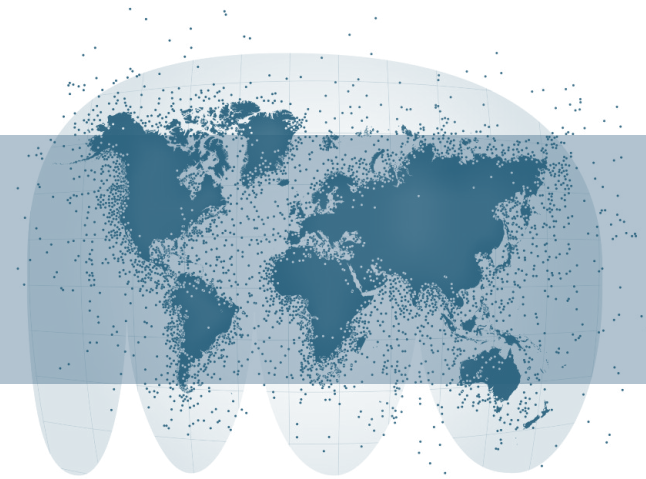
Tutto questo mi porta a chiudere il mio intervento mostrandovi un tramonto sull'orizzonte, perché è importante capire che la *cyber security* non è un obiettivo; non esisterà un giorno in cui potremmo definire il nostro Paese sicuro. Domani, cambierà la minaccia, cambierà la tecnologia, dovremo continuamente adattarci. E non sarà un adat-

tamento solo tecnologico, sarà un adattamento che partirà dalla normativa, passerà per nuove ri-organizzazioni e arriverà fino alla parte operativa.

In conclusione, lasciatemi porre questa domanda, la NIS è un punto di arrivo rispetto ad una perimetrazione per quanto riguarda la sicurezza cibernetica nazionale? Direi di no. Interi settori, a partire da quello governativo, a quello l'agroalimentare, fino alla difesa e allo spazio, sono completamente fuori dal perimetro NIS. È importante che l'Italia, come altri Paesi, si doti di uno strumento che permetta di avere un controllo ancora più forte sui livelli di cybersicurezza raggiunti dalle organizzazioni che erogano servizi strategici per la sicurezza nazionale.

In questo momento questa protezione non l'abbiamo. E questo lo potete toccare con mano ad esempio nella pubblica amministrazione guardando le procedure degli appalti pubblici: le gare di beni e servizi ICT gestiscono la sicurezza cibernetica al massimo ribasso. Questo è un obiettivo su cui sta lavorando l'NSC. In questo momento in Italia ciò che abbiamo a livello di pubblica amministrazione sono le misure minime di sicurezza cibernetica emesse da AgID, peraltro non cogenti, che non ci danno alcuna garanzia per quanto riguarda la difesa effettiva di un perimetro di organizzazioni che sono strategiche per il funzionamento del Paese e per la sua sicurezza.

Dobbiamo andare oltre queste misure, presto.



La sovranità nell'era digitale

Sessione III

Giuliano Amato

Giudice costituzionale

Maurizio Molinari

Direttore de "La Stampa"

Coordina: **Licia Califano**

Componente del Garante per la protezione dei dati personali

Sessione III

La sovranità nell'era digitale

Licia Califano

Nell'affrontare una tematica così complessa e nell'introdurre i due illustri relatori inizio con una serie di domande: l'avvento del digitale coincide con il radicamento di un nuovo potere sovrano? Quali sono i contorni della sovranità digitale e quali sono gli strumenti del diritto per limitarle?

La sovranità esprime il potere, anzi si potrebbe dire che sovranità e potere sono fondamentalmente la stessa cosa. È la capacità regolativa del diritto, il ruolo ambizioso di fondazione, di legittimazione e contenimento del potere, svolto in particolare dal diritto costituzionale, a delimitare la sovranità garantendo la libertà.

Lo Stato di diritto nasce intorno all'idea della delimitazione del potere politico, in ragione della rivendicazione di una libertà costruita sulla legalità e sulla giustiziabilità dei diritti. È la legge, generale e astratta, lo strumento che servì per delimitare il potere del sovrano assoluto. E lungo questa strada si arriva alle Costituzioni rigide, alle carte sovranazionali e internazionali per la difesa dei diritti fondamentali.

Oggi il tema è quello che molti autori definiscono dell'erosione della sovranità; io preferirei parlare di progressiva relativizzazione del concetto originario di sovranità.

Forse questo è l'effetto proprio della costruzione multilivello dei diritti e della forza espansiva del diritto giurisprudenziale delle corti.

Proprio sul processo di trasformazione del concetto di sovranità - che qualcuno considera al tramonto insieme agli Stati nazionali - si innesta la rivoluzione digitale. Si è, dunque, portati a chiedersi se quella che si apre è una stagione nuova per il costitu-

zionalismo, dal momento che ci troviamo di fronte ad un nuovo potere sovrano.

Un nuovo potere che, esattamente come in passato, si trasferisce da una sede ad un'altra; un potere che non ha più caratteri necessariamente privati, pubblici, personali o collettivi, ma ha essenzialmente caratteri tecnici.

Un potere che fonda la sua legittimazione su competenze di carattere tecnico-scientifico e sulla capacità di implementazione tecnologica e di controllo delle informazioni che da tali sistemi derivano.

Il potere cambia sede e, con esso, la sovranità. Dallo Stato si trasferisce in mani ignote, sconosciute. E il problema non risiede tanto nel fatto che si parli di mani ignote (in fondo lo stesso concetto di sovranità popolare ci riporta ad un soggetto astratto), quanto piuttosto che sia un potere privo di regole e che fatica ad essere sottoposto ad esse.

Una nuova forma di potere sovrano che pone al giurista l'urgenza di comprensione del fenomeno e la conseguente elaborazione di nuove forme e strumenti di tutela idonei a fissare la misura del potere e a proteggere i diritti anche contro il nuovo sovrano.

Nel paradigma digitale fatto di *big data*, di Internet delle cose, di intelligenza artificiale, automazione di tutti i processi produttivi e comunicativi, l'incidenza sulla sfera individuale, quindi su dignità e libertà dell'uomo da parte dei detentori di queste conoscenze tecnologiche può manifestarsi in molti modi: dai sistemi che generano un controllo a distanza dell'individuo lavoratore all'informazione connessa al corredo genetico di ciascuno di noi, alla profilazione, piegata alle finalità elettorali e politiche (il caso che tutti conosciamo di Cambridge Analytica), alla massiva raccolta di dati sanitari connessi a dispositivi medici che diventano un patrimonio economico inestimabile per le aziende farmaceutiche e le compagnie assicurative.

Non solo il progredire tecnologico sembra sfuggire alle forme conosciute di regolazione giuridica, ma se si guardano meglio i tratti di questo nuovo sovrano digitale, scavando oltre l'immagine dell'in-

novazione come fattore di sviluppo e di liberazione della persona, si scopre una dinamica interna mirata ad una crescita esponenziale e ad una sua diffusione che si mostra insofferente all'idea di limitazioni.

Quindi, come si governa la tecnologia digitale? Io credo che occorra partire dalla confutazione in radice della tesi della crescita lineare della tecnologia. A tal proposito richiamo Paolo Grossi: è "mitologia giuridica della contemporaneità" l'idea di una crescita lineare del rapporto tecnologia/libertà, tecnologia/democrazia, democrazia/cittadinanza. Di pari passo la consapevolezza dell'enorme concentrazione economica che la potenza di automazione e di rielaborazione ha prodotto nelle mani di soggetti privati.

Nell'affidare questi brevi spunti di riflessione ai relatori, mi chiedo anche quanto il nuovo regolamento generale sulla protezione dei dati possa essere letto come una risposta ovvero uno strumento idoneo in qualche modo a rispondere agli interrogativi posti all'inizio.

Si intrecciano all'interno del regolamento, a mio avviso, tre profili che possono rappresentare degli efficaci strumenti di regolazione e di tutela.

In primo luogo, l'impiego di una fonte normativa sovranazionale, capace tanto di uniformare quanto di lasciare spazio all'implementazione in ambito statuale.

In secondo luogo, la positivizzazione e la conseguente giustiziabilità tanto del principio di responsabilizzazione quanto dell'istituto della valutazione di impatto preliminare. Entrambi questi istituti, già testati in materia ambientale, chiamano in causa i soggetti privati che sono tenuti a definire e giustificare i limiti della propria azione.

Da ultimo, l'aver affermato la natura di diritto fondamentale della protezione dei dati personali.

Assistiamo così, forse - ma questo lo domando ai miei ospiti - ad un percorso circolare dei diritti fondamentali.

Da antidoto alla sovranità statale, a grimaldello per il suo superamento e oggi nuovamente antidoto, ma stavolta alla sovranità digitale?

Giuliano Amato

Parliamo di sovranità con una certa approssimazione ormai, perché di sicuro non è più quella che era. Se avessimo invitato qui Altiero Spinelli, gli si sarebbero rizzati i capelli, perché chi visse la Seconda guerra mondiale e le sue tragedie identificò nella sovranità degli Stati il nemico da eliminare. Ad essa si attribuiva la conflittualità divenuta armata e divenuta tragedia per milioni di esseri umani e quindi i federalisti europei, preceduti da Luigi Einaudi e da tanti altri, dissero "basta con la sovranità!". Questo "basta" aveva un elemento ideologico dentro di sé, l'elemento risalente all'origine della sovranità degli Stati nazionali, da Bodin ad altri: la sovranità come espressione di un potere che si autolegittima e che non accetta dimensionamenti da parte di altri, "*superiorem non recognoscens*".

Tutta l'organizzazione internazionale del nostro tempo e, in particolare, l'organizzazione sovranazionale che abbiamo noi in Europa sono fondati sul principio opposto del "*superiorem recognoscens*", sia pure un superiore fatto da me o fatto anche da me, e prerogative un tempo sovrane dello Stato sono state via via trasferite ad organizzazioni di livello superiore.

Che cosa è rimasto del potere sovrano di un tempo? È rimasto che ciascuna comunità nazionale si aspetta di essere difesa nei propri tratti identitari essenziali e nella propria esistenza in primo luogo dall'organizzazione pubblica che si è data. Ciascuno Stato ha un dispositivo militare e il dispositivo militare esiste nei Paesi democratici che accettano i nostri principi per difendere quella comunità da aggressioni esterne, che ne possano mettere in dubbio la sopravvivenza totale o parziale. Tutti ne sentono il bisogno, quindi questa cosa è rimasta: non esiste fenomeno ultra nazionale che abbia cancellato questa parte non eliminabile di ciò che un tempo chiamavamo sovranità, che è un principio giuridico ed è un principio fattuale; per noi giuristi qui valgono le regole dell'effettività: fino a quando lo sei? Fino a quando non arriva l'Armata Rossa, seguita anche dagli Alleati, che trasforma Berlino in una "*res nullius*". A quel punto la tua so-

vranità non c'è più. E non perché una legge superiore sia prevalsa sulla tua, ma perché la forza di altri è stata superiore alla tua. Quindi c'è questo elemento che dobbiamo tener presente, ed è nel mondo di oggi in realtà l'elemento che conta di più, perché non ci sarà nessuno che dirà che questo o quel Paese è legalmente soggetto ad un altro; appartiene a un mondo che non è più il nostro. Ma ci sarà chi si porrà il problema (e magari lo risolverà anche) di assoggettare parti rilevanti della vita di un Paese a qualcosa che non è espressione di quel Paese, il che può accadere nell'economia e, ciò che ha reso particolarmente inquietante la vita del nostro tempo, anche nell'assetto politico istituzionale: l'intervento nei processi elettorali di altri Paesi.

Questi sono i fenomeni che portano a dire in linguaggio non giuridico che esistono Paesi a "sovranità limitata"; siamo tutti ormai a sovranità limitata, ma, quando usiamo questa espressione, intendiamo dire che il nostro Paese, o un altro Paese, dipende (e non dovrebbe dipendere) da qualcosa che sta fuori.

La digitalizzazione ha favorito enormemente questi processi, che in realtà ci sono stati anche in passato, ma in forme e con capacità di successo e di penetrazione molto più basse. Per questo qui ci sono dei problemi. Dicevo inquietanti e dico inquietanti, perché non ci è molto chiaro ancora come potremmo risolverli. Ma non c'è dubbio che c'è chi ha interferito con le elezioni negli Stati Uniti e ha attentato a ciò che nei nostri ordinamenti è rimasto sovrano, al di là dello Stato: il suo singolo cittadino e la sua volontà. Tutto il mondo digitale tende a sottrarre il cittadino alla regola base degli ordinamenti democratici: confrontare opinioni diverse e scegliere tra queste. Il mondo digitale tende alla creazione di enclave che si chiudono ciascuna in se stessa e che tendono a far arrivare a ciascuno opinioni confermative di ciò che si presume questo ciascuno abbia già nella testa, in modo che non dubiti mai di ciò che, in base a giudizio o a pregiudizio, ha comunque già prescelto.

Il tema è quello qui già trattato e cioè che tutto questo avviene utilizzando dati personali. Sia in economia sia in politica. E noi ci muoviamo tra principi opposti. I dati personali? I dati personali de-

vono essere trasparenti. Ma allora, se devono essere trasparenti, come faccio a difenderli? Il principio della trasparenza fino a quale punto può valere per rendere ostensibili i dati miei, suoi, a fini economici o ad altri fini? A chi appartengono i dati? Se io sono addetto alla sicurezza nazionale, io ho disperato bisogno di dati, io li devo avere.

Io ho fatto il ministro dell'interno, so che cosa significa espellere dal Paese una persona che non ha commesso un reato, ma che potrebbe commetterlo, e gravissimo; so che, per adottare una decisione del genere, riuscendo dopo anche a dormire, tu devi avere acquisito dei dati su quello che questo personaggio è venuto facendo e quindi potrà fare. Questi dati non te li ha forniti lui, hai avuto bisogno di apparati funzionanti che te li hanno procurati. È giusto che sia così, è giusto che io, che ho una responsabilità che mi ha dato la mia collettività, disponga di apparati che sono in condizione di procurarsi questi dati destinati a me, quindi al Parlamento al quale io rispondo.

Ma possono questi dati essere disponibili per chiunque altro che li ottiene non per la sicurezza nazionale, ma per l'insicurezza nazionale? Posso io fare in modo di renderli acquisibili da lui, ma non acquisibili da altri che non hanno la stessa missione? Qui siamo davanti a questioni che dovremo affrontare con la consapevolezza di tutti gli elementi del nostro problema.

Parliamoci chiaro, il GDPR ha affermato finalmente il principio della portabilità dei dati nei confronti dei *provider*, ma dei dati forniti da ciascuno, non di quelli elaborati dal *provider* su ciascuno, di cui il singolo non ha diritto di sapere nulla. Anche l'interpretazione che si dà dei dati forniti è un'interpretazione piuttosto ampia.

Ci sono persone che forniscono tutto e della cui *privacy* io sono indotto a disinteressarmi totalmente, perché persone che fanno tutto in *Facebook*, poi pretendono pure che qualcuno tuteli la loro *privacy*.

Caro Antonello, a questi puoi dire "sii un po' più moderato".

C'è un'incontinenza che neanche Lines Notte potrebbe assorbire tutta, figuriamoci la rete! Quindi esiste un po' questo con-

trasto tra l'aver reso pubblica la propria vita e poi magari si dice "ma c'è l'articolo 15 della Costituzione!". Povera creatura l'articolo 15 della Costituzione, in questo clima si guarda intorno non capendo più di che cosa si dovrebbe occupare. C'è dunque anche il tema: la difesa dei propri dati dipende anche dalla disponibilità che ciascuno di noi ha a renderli disponibili. Però c'è il dato dall'altra parte. La nostra Corte ha davanti (la sentenza è già stata deliberata, ma non è stata ancora scritta) un caso delicato, di cui anche voi vi siete occupati, che è quello dei dati reddituali e patrimoniali di coloro che sono definiti dirigenti pubblici, sia che siano dirigenti apicali sia che siano medici del Servizio sanitario o dirigenti scolastici (circa centocinquantamila persone) più affini e parenti stretti e, in nome della trasparenza, si prevede che le amministrazioni non solo acquisiscano questi dati, ma li collochino in modo tale che qualunque motore di ricerca li possa acquisire e utilizzare ai fini suoi. In Italia come in Indonesia.

Ecco che qui c'è un problema di bilanciamento. Si può, in nome delle esigenze della trasparenza e della lotta alla corruzione, arrivare sino a quel punto nel rendere disponibili i dati personali? È una domanda. La risposta alla prossima puntata. Per ora posso formulare solo la domanda.

Certo, se penso alla sentenza della Corte del Lussemburgo che aprì la questione con gli Stati Uniti (il famoso caso Schrems del 2015) vige ormai il principio che fornire i dati a un Paese che non offre le stesse garanzie di protezione che offrono i nostri Paesi europei va oltre a ciò che l'articolo 8 della nostra Carta consente.

È una cosa seria in Europa la tutela dei dati personali e notate che la ragione di quella vicenda del caso Schrems era la sicurezza; io per la verità avevo collaborato al mio tempo proponendo di darli questi dati, ma la Corte ha ritenuto che fossimo andati troppo in là e che quindi, quando c'è un diritto fondamentale da una parte, c'è un'esigenza pubblica, sia pure importante, dall'altra ci deve essere un limite, e io vi confesso che non mi dispiace ci sia il limite. A che servono i servizi di *intelligence*, se poi tutti i dati personali sono così

reperibili ovunque? Basta fare un clic. Vogliamo arrivare a questo punto? Non è più il tempo di Mata Hari, non posso più vivere le avventure che negli anni Venti lo spionaggio mi permetteva di vivere, ma, se c'è uno spazio nel quale qualcuno può entrare, perché si è specializzato nel farlo, lasciamoglielo! Non rendiamolo uno spazio pubblico, un parco pubblico, un giardino in cui anche un bambino può prendere un dato riservato. Quindi forse la Corte del Lussemburgo aveva ragione.

Non voglio farla tanto lunga. Come si governa la tecnologia digitale? Anche a tutela della sovranità nazionale, si governa con regole sovranazionali. Non è pensabile di poterle regolare ciascuno per conto suo, perché comunque negli interstizi di regolazioni diverse si può infilare chiunque, ricavandone messe di benefici non dovuti. Quindi la miglior difesa della stessa sovranità nazionale è in regolazioni efficaci sovranazionali, che ci garantiscano una piattaforma comune. Poi vogliamo prima o poi (questo va oltre il diritto) applicare il principio che siamo sempre pronti ad enunciare, e cioè che non tutto ciò che è fattibile deve essere fatto? E vogliamo porre un alt a sviluppi tecnologici che possono dare luogo a dei risultati rovinosi? L'intelligenza artificiale nel militare, la sostituzione dell'essere umano con il robot sul campo di combattimento mi garantisce che io non avrò morti, ma a quali risultati potrebbe portare, se Charlie impazzisce? L'abbiamo visto in "Odissea nello spazio".

Siamo prossimi, se continuiamo così, all'odissea sulla Terra. Questo va evitato. Ci si può fermare, si può stabilire una regola per cui un numero rilevante di Paesi pone un limite all'uso dell'intelligenza artificiale in certi ambiti.

Io sono sempre rimasto convinto che, se questo fosse stato fatto alcuni decenni fa, forse non avremmo avuto gli ordigni che distrussero città giapponesi e che aprirono l'era dell'umanità che, anziché proteggere il pianeta in cui vive, lo distrugge e si mette in condizione di distruggerlo. È un errore che abbiamo fatto una volta, ci sono voluti decenni per accantonare gli ordigni nucleari, poi ora stanno tornando; ora ne stiamo inventando una che è anche peggio,

potremmo evitare di portare l'invenzione sino in fondo. Se noi rimaniamo un po' più intelligenti dei robot - dite la verità - è un po' una piccola soddisfazione, perché non tutti abbiamo la stessa intelligenza: quelli di noi che percepiscono di averne meno, almeno abbiano la soddisfazione di poter guardare i robot dall'alto in basso.

Maurizio Molinari

L'iniziativa del presidente del Garante per la protezione dei dati personali non potrebbe essere più attuale e più strategica: non solamente perché il recente *summit* di Davos ha trattato proprio questo tema a fondo, ma soprattutto perché il cuore delle sfide che abbiamo davanti nei prossimi due o tre anni hanno a che vedere con quanto il presidente Amato e, negli interventi precedenti, tanto Roberto Baldoni quanto Stefano Mele hanno indicato: la sfida dell'intelligenza artificiale.

Tentiamo di capire qual è la sfida che l'intelligenza artificiale pone alla sovranità nazionale e come può essere affrontata.

Perché è una sfida. Perché, come la rivolta delle tribù contesta la competenza degli Stati, come il jihadismo fa implodere gli Stati, come le rivolte populiste nei Paesi e nelle democrazie avanzate chiamano in causa la democrazia rappresentativa, così le comunicazioni digitali creano un sistema di comunicazione non governabile ed esterno agli attuali sistemi di rappresentanza e all'attuale sistema normativo. Quindi la minaccia è strategica. A questa minaccia la NATO reagì con il summit di Lisbona, suggerendo agli Stati di darsi dei *cyber command*, gli Stati membri si sono dati dei *cyber command* (incluso il nostro); abbiamo delle protezioni, chi più sviluppate, chi meno sviluppate, ma sicuramente oggi è un valore condiviso, non a caso le interferenze maligne - come sono state definite da uno degli ultimi Consigli atlantici - relative alle intrusioni da parte di altri Stati sono nell'agenda della sicurezza comune.

Ma questo è il tema che riguarda la sicurezza.

La sfida è il governo. Dal primo gennaio 2016 ad oggi sono stati prodotti più dati di quanto l'umanità abbia prodotto dall'inizio del mondo al 31 dicembre 2015. Significa che il numero di dati e di informazioni di cui stiamo parlando si moltiplica a una velocità superiore alla nostra immaginazione.

Questo porta alla sfida del come si governa e chi possiede i dati. Ci sono due modelli al momento esistenti: uno è il modello americano e l'altro è il modello cinese. Il modello americano si basa su grandi *corporation*, in gran parte (ma non solo) di stanza nella West Coast, che dispongono delle reti che hanno i dati, possiedono i dati. I dati sono loro, perché hanno le reti. Il modello cinese è che invece a possedere le reti è lo Stato. Questi sono i due modelli che esistono al momento. Entrambi hanno delle evidenti vulnerabilità. Nel primo caso consentono a grandi *corporation* di sfruttare i dati per declinare i propri interessi economici, nel secondo caso consentono a uno Stato di possedere una mole agghiacciante di dati su oltre un miliardo di persone.

Perché tutto ciò riguarda l'intelligenza artificiale, perché questa è la sfida sull'intelligenza artificiale? Che cos'è l'intelligenza artificiale? È l'applicazione delle nuove tecnologie su una massa di dati per riuscire a elaborare i dati e a sviluppare dei programmi che anticipano i ragionamenti degli esseri umani. Quindi più dati uno possiede, più può accelerare lo sviluppo dell'intelligenza artificiale.

Quindi la sfida in questo momento è fra questi due Paesi, perché, oltre a possedere le tecnologie, possiedono le reti che usano i dati. Perché in questa sfida è in vantaggio la Cina? Per due motivi. 1. ha sviluppato una tecnologia identica a quella degli Stati Uniti, ma è più a basso costo, quindi disponibile sul mercato a prezzi più agevoli; 2. ha a disposizione più dati. Avere a disposizione ventiquattro ore al giorno tutti i dati prodotti da oltre un miliardo di persone significa avere una banca dati, un arsenale di informazioni che nessun altro sul pianeta ha. Quindi ogni giorno che passa il vantaggio della Cina aumenta, perché ogni giorno loro, con la stessa tecnologia che hanno gli americani, lavorano su più dati. Quindi

nella corsa all'intelligenza artificiale il vantaggio cinese è strategico ed è destinato ad aumentare.

Questo è dove noi siamo. Siamo in questa situazione.

C'è un modello europeo? Questo è l'interrogativo. E quale può essere la strada dell'Europa in questa cornice. Sicuramente la normativa che il Parlamento europeo ha iniziato a esaminare, approvare e rafforzare disegna un approccio differente, che ha a che vedere con la protezione degli utenti. Il punto di inizio non è l'interesse delle grandi *corporation*, non è l'interesse dello Stato, ma è la protezione dell'utente. Non è *top-down*, è *bottom-up*. Quindi sicuramente fino a questo momento quanto il Parlamento europeo sta facendo è positivo e rivoluzionario, ma soprattutto risponde allo spirito europeo: la protezione dei diritti dei cittadini, ed è un approccio alternativo agli altri due. È chiaro che la debolezza del posizionamento dell'Europa è che forse, ad eccezione della Germania, sul fronte delle nuove tecnologie siamo in drammatico ritardo rispetto agli altri due concorrenti. Non siamo solamente in drammatico ritardo, ma, poiché il mercato è globale, alcuni dei nostri Paesi, alcune delle nostre aziende tendono inevitabilmente ad essere attirati dall'acquisto di reti che appartengono ad altri, e il duello non è più sulla tecnologia ma è sulla rete. Chi dispone della rete, dispone dei dati.

Quindi la sfida è chi costruisce le reti.

Perché tutto ciò ha tempi molto stretti? Perché la tecnologia, ad esempio per le auto che si guidano da sole, è oramai di fatto a disposizione, è solamente una questione di tempo, ma le macchine potranno andare su strada, quando ci sarà il 5G. Che cos'è il 5G? È il motivo per cui il CEO di *Samsung* ha il nuovo cellulare che si piega dentro la sua cassaforte a Seul e non lo tira fuori. Il 5G è una dimensione dello scambio delle comunicazioni digitali che annulla e polverizza tutto quello che oggi noi conosciamo. Significa che, attraverso gli strumenti che oggi noi abbiamo (gli *iPod*, gli *iPhone*, le tv digitali, eccetera), sarà possibile scambiare più dati ad una velocità più rapida e sostanzialmente ogni schermo diventerà tridimensionale. Significa che sarà possibile guidare una macchina come oggi avviene per un

jet militare. L'F-35, che è l'aereo più sviluppato del mondo, che è una centrale elettronica in grado di condurre molteplici operazioni, non solamente gli attacchi sul territorio, ha la stessa tecnologia che il 5G consentirà ad ogni cittadino di gestire. Tutto questo comporta una rivoluzione epocale. Perché la *Samsung* ha il cellulare flessibile? Perché è questo il punto vero: noi avremo uno schermo attraverso il quale fisicamente potremo avere la sensazione di toccare chi sta dall'altra parte. Tutto ciò non è lontano cinque anni, e probabilmente non è lontano neanche tre anni, quindi l'esigenza per l'Europa di darsi protezioni normative dei singoli cittadini, dei singoli suoi abitanti è drammaticamente impellente, perché la realtà è che noi siamo di fronte ad un processo dove l'innovazione tecnologica corre ad una velocità tale da mettere in affanno le istituzioni democratiche. Le istituzioni democratiche hanno una loro velocità di sviluppo, e l'Occidente orgogliosamente ha questa *leadership*, ma che assolutamente non è paragonabile allo sviluppo della nuova tecnologia. Quindi bisogna porsi l'interrogativo di come armonizzare tali due sviluppi.

Non si può fermare lo sviluppo dell'intelligenza artificiale, semplicemente perché è già fra noi, ma lo si può governare o si può iniziare in maniera diversa a proteggere, in maniera più corposa e più efficace, i diritti dei cittadini. Questa è la sfida. Giustamente il professor Amato faceva riferimento alla necessità di regole sovranazionali e di avere una piattaforma comune per difendere la sovranità degli Stati, e quindi i diritti dei cittadini, e qui un suggerimento lo dà Alan Dershowitz, il giurista liberal di Harvard. Cosa dice lui in questo libro fantastico «*Rights from wrongs*»? Che i diritti nascono dalla violazione dei diritti; più la violazione dei diritti è clamorosa e brutale, più le società democratiche sanno esprimere dei diritti che proteggono gli individui. Il punto vero è che di fronte alla violazione massiccia dei diritti degli individui nella realtà digitale (le *fake news*, l'odio, il bullismo e quant'altro la realtà digitale consente di violare i diritti del singolo), la sfida è di creare delle protezioni digitali. Il che significa, parlando sulla base del diritto europeo, declinare nella realtà digitale il nostro Stato di diritto. Questa è la sfida. Lo Stato di

diritto non va cambiato. Lo Stato di diritto che le democrazie occidentali hanno è lo strumento più formidabile per garantire la convivenza degli esseri umani. Il punto è che deve essere declinato nella realtà digitale. Per declinare lo Stato di diritto nella realtà digitale servono nuove norme che devono essere sovranazionali, devono essere europee, ma devono essere implementate ad una velocità formidabile, perché l'intelligenza artificiale non aspetta.

Questa è la sfida che abbiamo di fronte a noi, è giusto vederla nella sua drammaticità e affrontarla senza alcuna remora.

I Confini del Digitale

Nuovi scenari per la protezione dei dati

Conclusioni

Giulia Bongiorno

Ministro per la Pubblica Amministrazione

Conclusioni

I Confini del Digitale Nuovi scenari per la protezione dei dati

Intervento di Giulia Bongiorno
Ministro per la Pubblica Amministrazione

Buongiorno a tutti. Porgo questo saluto anche a nome del sottosegretario Giorgetti e tengo a precisare che l'assenza è dovuta non a scarsa considerazione per il tema - che è al contrario una delle priorità del sottosegretario e di tutto il governo - ma alla concomitanza con un funerale di Stato.

Considerato che abbiamo dei tavoli aperti anche con il sottosegretario, ho ritenuto di potervi portare il suo saluto e qualche breve considerazione. Ho ascoltato soltanto gli ultimi due interventi, perché in contemporanea avevo un altro impegno, parto comunque dal titolo del convegno che mi sembra lanci una bella provocazione: ci si chiede quali possano essere i confini del digitale e sembra quasi una contraddizione in termini, perché il digitale è sconfinato. Nel secolo scorso tutti pensavamo alla rivoluzione che avrebbe portato il petrolio, oggi la rivoluzione è una rivoluzione di dati. Condivido in pieno quanto diceva Molinari: la ricchezza è collegata al dato, e di questo non c'è consapevolezza. Come non c'è consapevolezza della ricchezza che questi dati possono generare. Forse in questa sala, dove siete più o meno tutti del settore, ce n'è piena consapevolezza, ma vi assicuro che fuori di qui è diverso.

Condivido anche quanto si diceva sui dati degli ultimi tempi, perché anch'io ho dei numeri: il novanta per cento dei dati immagazzinati nei sistemi è stato prodotto negli ultimi due anni. Questo deve far riflettere: se tanto mi dà tanto, la velocità è destinata ad aumentare e, quindi, avremo un numero di dati sempre maggiore.

Nei prossimi cinque anni, secondo le previsioni ci saranno un miliardo di nuovi utenti e cinquanta miliardi di nuovi dispositivi.

Anche questi numeri secondo me devono far riflettere.

Ecco perché dicevo che il titolo del convegno contiene una provocazione. Verrebbe da dire che, se stiamo parlando di un universo - perché quello digitale è un universo -, è difficile non solo stabilire dei confini ma anche, come dicevano il professor Amato e Molinari, disciplinare questo universo con una legge nazionale.

È ridicolo soltanto pensarlo.

Cosa si dovrebbe fare? Parlare di digitale, spiegare cos'è, qual è la ricchezza che ne deriva, e che sfugge a molti. Sfugge, secondo me, anche ai nostri figli. Perché gli utenti, in particolare i giovanissimi, tendono a dare informazioni senza curarsi della privacy. L'app *Economy*, in continua crescita, si basa proprio su questo: offre una serie di servizi in cambio di dati. Ma chi dei nostri figli pensa di stare "cedendo" qualcosa? L'obiettivo dei giovani è ottenere il prodotto.

Scrivere "mi chiamo Nicola Rossi" non viene percepito come una cessione di dati. Anche a me è successa una cosa simile. Insieme a Michelle Hunziker ho dato vita a una fondazione che tutela le donne vittime di violenza: ci sono state offerte gratuitamente delle app che avremmo dovuto dare alle nostre assistite. Io la trovavo una cosa straordinariamente utile e mi chiedevo come mai volessero darcela gratis.

Finché un giorno una persona, forse più trasparente di altre, mi ha spiegato perché: nel momento in cui le singole fondazioni e associazioni offrono alle donne questa app per difendersi, il proprietario dell'app immagazzina gratuitamente i dati. È importante spiegare queste cose! A voi sembrerà quasi banale, ma sappiate che fuori da quest'aula non lo è affatto! E mentre noi parliamo, i dati viaggiano velocemente, li stiamo regalando. Anzi, addirittura ora c'è questa nuova app, *Killi*: gli utenti sanno che i loro dati vengono venduti e li vendono ben volentieri, monetizzano e via! Insomma: siamo sicuri che ci sia consapevolezza del valore dei dati?

Detto questo, mi sembra un bene che l'Unione europea abbia emanato la normativa GDPR, ma adesso ci vuole uno sforzo maggiore, uno sforzo che dovrebbe essere direttamente proporzionale all'importanza della sfida che avete illustrato prima, in cui si intrecciano numerosissimi aspetti: la sicurezza (che credo sia stato trattato prima di me); la privacy; il tema economico; il diritto penale, perché in questa vicenda vi sono anche profili penali. Ricordo un caso interessantissimo e controverso, quello di *Vivi Down*: c'era un video in cui un ragazzino down era stato ripreso e ridicolizzato dai compagni di classe. Il video era stato girato da un ragazzino, caricato in rete da un altro e poi messo in circolazione da Google video, il cui server però era non in Italia ma in America. Quindi si creava un enorme problema, anche di responsabilità rispetto a questi dati: avevamo un server in America, una parte di responsabilità in Italia e il famoso tema di cosa fanno esattamente i motori di ricerca: se davvero, cioè, il ruolo sia di semplice intermediazione - come loro spesso sostengono, per cui ci si limita a prendere un dato e a diffonderlo - , o se invece, come in quel caso sosteneva l'accusa, non basta prendere un dato, perché esiste la responsabilità, ex articolo 40, secondo capoverso, del codice penale, che è la cosiddetta "omissione impropria", ovvero: il soggetto che ha una posizione di garanzia non può restare immobile, fermo, omissivo. Deve attivarsi. Se io ho dei dati sensibili, non posso dire "mi limito a trasmetterli, cosa posso farci? "Io divento *garante* di quei dati. È stato, credo, uno dei processi più significativi, almeno nel campo penale: fu seguito anche in Italia, perché non si sapeva più bene che normativa applicare - i dati erano a Denver, ma la condotta era stata parzialmente realizzata in Italia.

Tutto questo per dire che sono d'accordo con voi: non si può fare una legislazione italiana, sarebbe ridicolo. Ma vi dirò di più.

Non può essere nemmeno una legislazione europea. Io vado oltre, perché quando mi trovo delle realtà in America, la nostra legislazione europea quantomeno dovrà prevedere una serie di princìpi, norme e regolamenti che consentano anche di stabilire, prevedere e regolare cosa accade fuori dall'Europa. Stiamo parlando di un universo.

Veramente fa quasi sorridere chi pensa (e io l'ho pensato) di poter parlare di Italia.

Voi sapete che sono ministro per la Pubblica Amministrazione e che ho la delega per il digitale: quando ho cominciato ad affrontare questi discorsi, mi sono ritrovata a tavoli in cui mi dicevano: "Ministro, noi siamo già a posto, perché esiste il CAD". Il CAD è il Codice dell'Amministrazione digitale, che secondo me è la dimostrazione di come non si debba legiferare. Pensate che all'interno del CAD ci sono norme che contengono formule tecnologiche già superate. Non c'è più il codice che viene abrogato da un'altra norma, ma la tecnologia che supera la norma. Pensare che un CAD possa esaurire il problema significa pensare di poter far entrare il mare in una buca scavata sulla spiaggia. Il CAD è semplicemente uno strumento, che oltretutto secondo me va rivisto: diciamo che si tratta di un punto di partenza.

Ma non voglio codici che contengano richiami tecnologici, perché, già mentre li scriviamo, veniamo superati da altre formule. Questo è un dato oggettivo.

Le ultime considerazioni riguardano il mio "ministero", in particolare il dipartimento della funzione pubblica e il digitale. Io sto cercando di valorizzare al massimo l'AgID, oggi considerata una realtà minore. Sono contenta di aver nominato Teresa Alvaro, che ha esperienza nella Pubblica Amministrazione e in materia di digitalizzazione.

Sapete qual è l'età media del dipendente nella pubblica amministrazione? Cinquantadue anni, cinquantasei per i dirigenti. Io credo che se al ministero chiamassi mio figlio, che di anni ne ha appena otto, avrebbe un'attitudine probabilmente migliore di un cinquantaduenne. Non perché a cinquantadue anni siamo vecchi, ma perché c'è un altro dato oggettivo: in certe cose, chi è giovane riesce meglio.

Cosa bisogna fare? Io sto cercando di fare molta formazione. Nell'ambito della Pubblica Amministrazione dobbiamo fare formazione per il digitale, altrimenti avremo pubblici dipendenti e diri-

genti che lo metteranno da parte, ancora oggi gira troppa carta. Tutti chiedono cosa succederà, se arriverà il digitale: secondo me, sarà una rivoluzione. Ma se in Gran Bretagna ci hanno messo dieci anni, noi, che stiamo partendo da zero, non possiamo pensare di riuscirci in poco tempo. È chiaro, dobbiamo porci anche dei problemi di privacy - e su questo avremo la collaborazione del Garante -, perché una trasformazione digitale richiede di contemperare queste esigenze.

Credo però che, per trasformare la Pubblica Amministrazione con il digitale, sia necessario partire da un dato: chi di voi ha chiesto una carta d'identità a Roma ultimamente, da quando c'è la carta d'identità digitale, purtroppo la riceverà dopo quattro mesi; in alcuni comuni, invece, può anche riceverla subito. Eppure il prodotto elettronico è uguale. Come mai, allora, tempistiche così diverse? Perché noi possiamo digitalizzare il mondo, ma se prima non semplifichiamo le procedure, se prima non organizziamo bene il personale e gli uffici - con un occhio anche alla tutela della privacy - avremo quello che succede spesso in Italia: i ministeri con una serie di dubbi. "Ma questo si può fare o c'è un problema di privacy?".

Cosa ho fatto io? Ho cercato, nell'immediatezza, di diramare una circolare (la n. 3), in cui chiedo una cosa banale, che forse si sarebbe dovuta fare molti anni fa: visto che dobbiamo contemperare la privacy con il digitale, visto che ci sono normative da fare, gradirei che nella Pubblica Amministrazione ci fosse un responsabile della transizione digitale, perché se non so nemmeno con chi devo interloquire, se nei ministeri non c'è questa figura, non si può andare avanti. Se dico che siamo all'anno zero, è appunto perché mi sono ritrovata in un ministero in cui non era ancora pronta la circolare sul responsabile della transizione digitale. Questo non perché non sia stato fatto niente, ma perché la trasformazione digitale richiede oltre al tempo anche regole agili, e non enormi CAD.

Regole agili e consapevolezza dei ruoli.

Siamo di fronte all'universo: regoliamolo, ma senza credere di poter fare tutto in casa.

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Redazione
Garante per la protezione dei dati personali

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

A cura del
Servizio relazioni esterne e media

Stampa:
UGO QUINTILY S.p.A.