COMMISSIONE PARLAMENTARE PER LA SEMPLIFICAZIONE

RESOCONTO STENOGRAFICO

INDAGINE CONOSCITIVA

14.

SEDUTA DI LUNEDÌ 25 MAGGIO 2020

PRESIDENZA DEL PRESIDENTE **NICOLA STUMPO**

INDICE

PAGINA BIANCA

PRESIDENZA DEL PRESIDENTE NICOLA STUMPO

La seduta comincia alle 10.30.

Sulla pubblicità dei lavori.

PRESIDENTE. Avverto che la pubblicità dei lavori della seduta odierna sarà assicurata anche attraverso la trasmissione televisiva sul canale satellitare della Camera dei deputati e la trasmissione diretta sulla *web-tv* della Camera dei deputati, anche per consentire ai deputati e ai senatori che non hanno potuto essere presenti di seguire i nostri lavori.

Audizione del presidente dell'Autorità Garante per la protezione dei dati personali, Antonello Soro.

PRESIDENTE. Gentili colleghi, dopo la sospensione dei nostri lavori a causa delle misure di contenimento dell'emergenza sanitaria da Covid-19, riprendiamo con la riunione odierna lo svolgimento del programma di audizioni previsto nell'ambito dell'indagine conoscitiva sulla semplificazione dell'accesso dei cittadini ai servizi erogati dal Servizio sanitario nazionale, che stiamo svolgendo ormai da alcuni mesi.

Prima di procedere all'audizione all'ordine del giorno, vorrei dare alcune brevi comunicazioni. I Presidenti delle Camere hanno autorizzato la richiesta di proroga del termine per la conclusione dell'indagine, che è quindi aggiornato al prossimo 31 luglio, e hanno altresì autorizzato la richiesta di alcune integrazioni del programma di audizioni. Nelle ultime due settimane l'Ufficio di presidenza, integrato dai rappresentanti dei gruppi, si è riunito per individuare una modalità di lavoro che ci consentisse di giungere rapidamente alla conclusione dell'indagine. In questa sede è stato stabilito di concludere lo svolgimento del ciclo di audizioni in corso attraverso quattro sedute, inclusa quella odierna, che, compatibilmente con i lavori delle due Assemblee, dovrebbero svolgersi il 1° giugno, venerdì 5 e lunedì 8 giugno prossimi. Nella prossima seduta avrà luogo l'audizione dei rappresentanti delle associazioni e delle cooperative per l'assistenza domiciliare, successivamente quella dei rappresentanti delle associazioni dei medici di medicina generale e dei farmacisti e infine una seduta sarà dedicata all'audizione di esperti selezionati sulla base delle vostre segnalazioni.

Secondo questo programma di lavoro avremmo quindi il tempo per definire la scaletta dei contenuti del documento conclusivo dell'indagine e procedere all'approvazione del documento stesso entro il termine stabilito del 31 luglio. Credo che l'obiettivo di portare a compimento nel più breve tempo possibile l'indagine stia particolarmente a cuore a tutti noi, anche alla luce della drammatica esperienza che il Paese sta attraversando, rispetto alla quale è diventato evidente ormai a tutti come la possibilità di fruire di servizi sanitari in modalità digitale sia anche fattore cruciale per affrontare efficacemente emergenze sanitarie.

Procediamo, quindi, all'audizione del presidente dell'Autorità garante per la protezione dei dati personali, Antonello Soro, che svolgerà da remoto una relazione sulle questioni relative al cosiddetto « diritto alla *privacy* » connesse all'attivazione del fascicolo sanitario elettronico, anche alla luce delle novità introdotte in proposito dal de-

creto-legge n. 34 del 2020, il cui esame è stato assegnato alla Camera la settimana scorsa. Naturalmente aggiungerei anche, se possibile, qualcosa rispetto all'*app* Immuni, che è vero che non è di stretta competenza della nostra Commissione, ma che ha dei collegamenti oggettivi per quelle che poi saranno le potenzialità del servizio sanitario sugli strumenti digitali.

Do quindi la parola al presidente Soro, che ringrazio innanzitutto per aver immediatamente aderito al nostro invito a partecipare ai nostri lavori, ricordando che al termine dell'intervento è previsto un breve spazio per le domande dei deputati e dei senatori presenti. In ragione dei tempi, ricordo sempre che, eventualmente, potremmo anche usare una formula che spesso abbiamo utilizzato, vale a dire far pervenire per iscritto le domande al presidente Soro per poi ricevere le risposte sempre per iscritto, in modo tale da poter utilizzare al meglio tutto il tempo del nostro lavoro. A lei la parola, presidente.

ANTONELLO SORO, *presidente dell'Autorità Garante per la protezione dei dati personali*, Grazie, presidente. Ringrazio la Commissione per questa occasione di confronto sul rapporto tra il diritto alla salute e la protezione dei dati, tema di grande rilevanza ma, in particolare, nell'attuale contesto emergenziale, di particolarissima importanza. Questi due diritti fondamentali presentano infatti inattese analogie, dovute essenzialmente alla dialettica che sottendono: fra libertà e dignità, persona e società. Questi diritti vivono poi in costante dialettica tra garanzia individuale e tutela sociale, realizzando la prima nel bilanciamento con la seconda, spesso persino in sinergia. Il rapporto tra libertà e dignità, individuo e società diviene ancora più articolato per effetto della tecnologia, che, se da un lato offre possibilità straordinarie, dall'altro induce nuove vulnerabilità cui, tramite i nostri dati, esponiamo noi stessi. Così in ambito sanitario la digitalizzazione è una componente essenziale di efficienza del governo clinico tale da garantire anche un'assistenza sanitaria personalizzata, fondata sulla partecipazione consapevole del paziente al percorso terapeutico. La pandemia ha dimostrato come il digitale, con la ricetta elettronica, con la telemedicina, possa consentire la prosecuzione delle cure anche in regime di distanziamento sociale.

Apro una parentesi molto breve sull'*app* Immuni, come il presidente mi ha richiesto, per rinviare alle considerazioni generali svolte in un'audizione parlamentare tenuta alcune settimane fa, ma anche per aggiornare sulle valutazioni più recenti. In questi giorni, in queste ore, sta per arrivare la documentazione relativa alla valutazione di impatto sulla *privacy* che il Ministero della Salute ha svolto sull'*app* Immuni, sulla quale per legge noi dovremo tempestivamente esprimere un parere conclusivo. Allo stato, la norma che il Governo ha inviato alle Camere è una norma che risponde alle richieste che avevamo fatto, non solo di scelta volontaria e di scelta preferenziale decentrata rispetto all'alternativa possibile di un accentramento dei dati. Non è prevista la geolocalizzazione, che era altro elemento che avevano sconsigliato, non solo perché è più invasivo dal punto di vista della protezione dei dati, ma anche perché meno efficace, nel senso che il perimetro di relazione fra i telefoni ai fini di un'individuazione del possibile contatto con altre persone del soggetto interessato alla ricostruzione della catena epidemica è molto meno specifico, perché riguardante un perimetro molto largo. Le interlocuzioni di queste settimane dovrebbero essere servite – me lo auguro – a rimuovere ogni ulteriore dubbio e a consentirci di potere con grande certezza, per quello che è possibile in questa materia, consigliare agli italiani di scaricare l'*app*. Lo valuteremo nelle prossime ore, nei prossimi giorni, non appena arriverà la valutazione di impatto conclusiva.

Tornando all'oggetto specifico dell'audizione odierna, la tecnologia, che in queste settimane ha offerto grandi opportunità agli italiani, e non solo agli italiani, di superare la limitazione delle relazioni personali fisiche, ha consentito di avere tutta una serie di altre opportunità. Ep-

pure la tecnologia non ben governata può aumentare il rischio clinico in cui si riflette in questo ambito, quello sanitario, il rischio informatico, ove, ad esempio, i dati su cui si fonda la diagnosi siano alterati. Per altro verso l'esfiltrazione o l'accesso indebito ai dati sanitari possono violare in modo talora irreversibile quel diritto all'intangibilità della propria vita privata che costituisce la radice più antica della *privacy*. Sul piano individuale, la conoscenza di dati così sensibili quali quelli genetici o sulla salute può fondare discriminazioni – si pensi al rapporto lavorativo o assicurativo – o comunque pregiudizi molto rilevanti per l'interessato, ma il rischio cibernetico in ambito sanitario ha effetti importanti anche dal punto di vista collettivo.

Sul piano pubblico, infatti, gli attacchi a sistemi informativi di strutture sanitarie, parte significativa dei *cyber attack* nel nostro Paese, possono avere effetti devastanti su tutti i cittadini, impedendo l'erogazione di prestazioni sanitarie o, nel caso di alterazioni dei dati dei pazienti, determinando errori clinici su larga scala. La vulnerabilità dei sistemi sanitari rischia quindi di causare disservizi anche gravissimi, generando errori diagnostici o terapeutici o paralizzando l'attività di cura. Sono state in questi anni diverse le esperienze in altri Paesi, in particolare in Inghilterra e negli Stati Uniti, in cui un attacco cibernetico molto devastante ha bloccato le attività di alcuni ospedali per settimane intere. È un problema, questo, che riguarda il nostro Paese in modo particolare. Recenti ricerche hanno indicato che il settore sanitario è uno di quelli esposti a maggiori rischi in termini di *cyber security*, perché carente di un piano organico di sicurezza e protezione che, invece, in questo campo sarebbe essenziale, soprattutto a fronte del sempre maggiore utilizzo del *cloud computing* e dell'intelligenza artificiale.

La sfida di oggi consiste allora nel rendere la digitalizzazione in ambito sanitario un processo organico lungimirante e sicuro, promuovendo così l'efficienza del sistema e, con essa, l'effettività del diritto alla salute, superando le vulnerabilità della tecnica e limitando i rischi individuali e collettivi. Il fascicolo sanitario elettronico è, in un certo senso, l'emblema di questa sfida quale elemento imprescindibile di innovazione ed efficienza delle attività diagnostiche e terapeutiche, previsto dall'Agenda digitale italiana ed europea, dal Patto per la salute, dal Patto per la sanità digitale e indicato quale piattaforma abilitante dal piano triennale dell'AGID (Agenzia per l'Italia digitale). Tuttavia, l'affidamento dell'intera storia clinica di milioni di pazienti a un'infrastruttura informatica rappresenta anche una non trascurabile fonte di vulnerabilità, se priva di protezioni adeguate a impedire accessi indebiti, esfiltrazioni o alterazioni dei dati. Questo spiega l'esigenza da noi in passato più volte sollecitata di una cornice normativa tale da dotare uno strumento tanto irrinunciabile quanto delicato di tutti i presidi necessari in termini di misure di sicurezza, ma anche di complessiva architettura del sistema. La previsione legislativa ha anche consentito di ricondurre iniziative regionali disomogenee all'interno di un quadro di garanzie uniformi tali da assicurare il pari trattamento dei cittadini.

Fin dal 2009, tre anni prima dell'introduzione della relativa disciplina, l'Autorità Garante ha fornito alcune importanti indicazioni sul fascicolo sanitario elettronico come del resto sul dossier sanitario, rilevando, in particolare, la necessità di garantire piena libertà al paziente sulle scelte essenziali relative al fascicolo, ivi incluse quelle inerenti la sua ampiezza e la possibilità di oscurare alcuni eventi clinici; la legittimazione selettiva e differenziata del personale autorizzato ad accedervi e il diritto del paziente a verificare gli accessi effettuati, restituendo così centralità all'interessato nel processo di gestione dei suoi dati; l'obbligo del titolare di segnalare all'Autorità Garante eventuali *data breach* occorsi nella propria struttura, quando ancora l'obbligo di notifica delle violazioni dei dati non era generale, così come oggi previsto dal nuovo regolamento europeo, al fine di contenere con misure tempestive i danni individuali e collettivi suscettibili di derivare da violazioni in questo ambito.

Queste indicazioni hanno consentito di migliorare notevolmente la qualità delle prestazioni erogate, ponendo le condizioni necessarie per promuovere la fiducia dei cittadini in uno strumento diagnostico essenziale ma ancora assai poco diffuso, in quanto attivato nei confronti del solo 23 per cento della popolazione.

Tale constatazione, unitamente al costante monitoraggio dell'applicazione normativa, ha quindi consentito di proporre, anche alla luce del sopravvenuto regolamento europeo, misure di semplificazione e al tempo stesso di valorizzazione del fascicolo sanitario elettronico, poi introdotte proprio dal cosiddetto « decreto-legge rilancio ». In particolare è stata ritenuta opportuna, e dall'Autorità Garante condivisa, l'eliminazione del consenso all'alimentazione del fascicolo, confermando invece quello, autenticamente espressivo di autodeterminazione informativa, relativo alla consultazione da parte dei professionisti sanitari. Tale modifica contribuisce a semplificare notevolmente il processo di costituzione del fascicolo, rendendolo quindi automaticamente disponibile a prescindere da manifestazioni di volontà individuali, ma confermando il consenso del paziente quale fonte di legittimazione dell'accesso ai dati da parte del professionista sanitario. Lo spettro del fascicolo è ampliato fino a comprendere tutti i documenti sanitari e socio-sanitari riferiti alle prestazioni erogate, a carico o meno del Servizio sanitario nazionale, includendo dunque tra i soggetti abilitati all'alimentazione la generalità degli esercenti le professioni sanitarie che seguono il paziente. La prevista ulteriore alimentazione del fascicolo con i dati disponibili sulla scelta circa la donazione degli organi, su vaccinazioni e prenotazioni promuoverà poi l'efficacia delle prestazioni sanitarie se e nella misura in cui garantirà l'allineamento delle banche dati e, quindi, l'esattezza e l'aggiornamento delle informazioni.

Si prospetta, inoltre, un notevole potenziamento, che dovrà essere oggetto di attento monitoraggio, del portale e dell'infrastruttura nazionale per l'interoperabilità, necessario all'erogazione delle prestazioni sanitarie in mobilità dei cittadini ovvero nell'ambito di regioni diverse da quelle di residenza. Si prevede, quindi, l'istituzione dell'anagrafe nazionale dei consensi e relative revoche, da associarsi agli assistiti risultanti dall'anagrafe, comprensiva anche dei dati inerenti a eventuali deleghe, ad esempio per le decisioni riferite a minori. La valorizzazione della funzione e l'estensione dello spettro del fascicolo prevista con il cosiddetto « decreto-legge rilancio », anche sulla scorta delle indicazioni fornite dall'Autorità Garante, rappresenta certamente una sfida importante per il settore sanitario da giocare fino in fondo, senza però sottovalutare in alcun modo i rischi connessi all'affidamento a una piattaforma informatica dei dati sulla storia clinica, potenzialmente, di tutti gli assistiti.

Per un verso, infatti, il rischio informatico, suscettibile di risolversi fatalmente in rischio clinico, va contrastato con la più rigorosa osservanza del principio di responsabilizzazione e dei criteri di *privacy by design* e *by default*, razionalizzando il patrimonio informativo e la stessa architettura del trattamento, seguendone la dinamica lungo l'intera filiera. Va anche inteso in senso rigoroso il vincolo di finalità, evitando l'accesso ai dati del fascicolo sanitario elettronico di cui difficilmente può garantirsi la completa anonimizzazione per fini di programmazione sanitaria da parte di amministrazioni titolari di competenze diverse. Su questo aspetto confido che le incomprensioni con il Ministero dell'Economia e delle finanze siano risolte, anche perché quel Dicastero già detiene dati fiscali rilevanti al monitoraggio della spesa anche in ambito sanitario. Del resto, già il Ministero della Salute utilizza il fascicolo sanitario elettronico ai fini, oltre che di ricerca, anche di programmazione sanitaria, verifica della qualità delle cure e valutazione dell'assistenza sanitaria – cosiddette finalità di « governo » – senza tuttavia l'utilizzo di dati identificativi o di documenti clinici, secondo livelli di accesso e modalità di elaborazione dei dati definiti in conformità ai principi di pro-

porzionalità, necessità e indispensabilità. Per altro verso, non va sottovalutato il rischio di accessi indebiti ai dati del fascicolo sanitario resi possibili da un'inadeguata definizione del perimetro e dei profili di legittimazione degli stessi professionisti sanitari. Non sono stati rari i casi, in questi anni sottoposti alla nostra attenzione, di consultazione dei fascicoli sanitari, da parte di persone prive dei titoli, per fini ritorsivi o di semplice patologica curiosità. La violazione della riservatezza derivante da tali condotte potrà essere poi persino più significativa ove nel fascicolo confluiscano dati di particolare rilevanza sotto il profilo delle scelte esistenziali, quali quelle sulla donazione degli organi o, laddove dovesse prevedersi, sulle dichiarazioni anticipate di trattamento. La protezione dei dati da accessi indebiti e l'esatta definizione dei soggetti legittimati alla consultazione costituiscono un obiettivo ineludibile soprattutto nel contesto sanitario complessivamente inteso. Si pensi alla delicatezza di dati quali quelli, pur non presenti nel fascicolo, sulla fecondazione eterologa, per i quali deve garantirsi, attraverso un sistema di codifica, tanto la tracciabilità del percorso dei gameti dal donatore anonimo al nato e viceversa, per consentire la reidentificazione in caso di eventi avversi, quanto la riservatezza delle madri. La gestione, poi, di tali dati così delicati e in costante evoluzione quali quelli sanitari necessita di garanzie idonee ad assicurarne la qualità. In questo senso, le regole di protezione dei dati sono un presupposto di efficienza sanitaria, contribuendo alla garanzia di esattezza e aggiornamento dei dati in un ambito, quale quello in esame, in cui il ricorso a un'informazione obsoleta o alterata può determinare danni talora anche letali per il paziente. L'aggiornamento costante deve del resto riguardare anche le manifestazioni di volontà dell'assistito per poterne garantire l'effettivo rispetto nella loro attuale evoluzione. È un tema che riguarda molti degli archivi rilevanti in questo campo. Esso coinvolge, infatti, il consenso alla consultazione del fascicolo, la cui anagrafe comprende anche appunto le revoche, ma, a maggior ragione, in ambito contiguo, le dichiarazioni anticipate di trattamento. Rispetto alle scelte sul fine vita, infatti, la centralizzazione delle dichiarazioni è necessaria per evitarne il disallineamento e, quindi, garantirne il costante aggiornamento necessario per il rispetto della volontà attuale del soggetto. Il processo di digitalizzazione in ambito sanitario, di cui il fascicolo è una componente significativa, pone del resto anche altre questioni rilevanti dal punto di vista della protezione dei dati, cui accenniamo, pur estendendo un minimo l'oggetto del nostro confronto di oggi.

Il ricorso sempre più frequente all'intelligenza artificiale ai fini di ricerca in campo medico, ma anche diagnostici, evidenzia l'esigenza di garantirne la correttezza nel processo analitico fondato sui dati, ove le scelte algoritmiche sono rese possibili dall'autoapprendimento di cui è capace la macchina, a partire dalle informazioni immesse. Dall'esattezza dei dati utilizzati nella configurazione degli algoritmi dipende l'intelligenza delle loro scelte. Se è errata la classificazione delle casistiche di riferimento fornita all'algoritmo per decidere, ad esempio, la natura di una patologia o per valutare un *marker*, sarà poi conseguentemente la diagnosi a essere sbagliata, con effetti potenzialmente anche fatali per il paziente. La protezione dei dati, dunque, è un presupposto di efficacia della *big data analytics* e va coniugata non certo con un arretramento ma, al contrario, con un ulteriore sviluppo di tecnologie *user-friendly* che incorporino in sé garanzie di sicurezza e confidenzialità dei dati.

Le misure di *privacy by design* e *by default* da applicare per esempio in modo rigoroso rispetto alla sempre più diffusa telemedicina sono in questo senso un esempio determinante di come la tecnologia, se sostenuta da una visione lungimirante in termini sociali, oltre che giuridici, possa rappresentare la soluzione del problema e rafforzare la fiducia dei cittadini nel sistema sanitario. Soluzione tanto più necessaria a fronte di ricerche sempre più fondate su dati e algoritmi idonei a incrociare

quantità enormi di informazioni, con un elevato rischio non soltanto di reidentificazione, che induce a ritenere i dati effettivamente anonimi solo in casi marginali, ma anche di discriminazione per gruppi, rischio tanto più elevato ove i *data set* sui quali si fonda la decisione algoritmica non siano rappresentativi o sottendano comunque pregiudizi di genere, etnia, condizione sociale o, appunto, di salute. La protezione dei dati può rappresentare tanto un elemento di garanzia del singolo, quanto un fattore di appropriatezza della generale *governance* sanitaria.

Sotto questo profilo, questa disciplina offre importanti garanzie esigendo in particolare trasparenza, contestabilità, non discriminatorietà del processo algoritmico, oltre che un approccio generale volto alla prevenzione del rischio, con la previsione di misure precauzionali e l'adozione di una strategia complessiva volta alla responsabilizzazione dei protagonisti del trattamento. Abbiamo ricordato questi principi anche rispetto ai sempre più frequenti modelli di assistenza sanitaria fondata sulla medicina d'iniziativa e, quindi, sulla profilazione del rischio sanitario e che, sebbene volti alla personalizzazione della medicina e al miglioramento dell'offerta terapeutica, coinvolgono tuttavia aspetti delicatissimi dal punto di vista esistenziale.

Garanzie di correttezza andranno assicurate anche rispetto all'uso, promosso dal cosiddetto « decreto-legge rilancio », di metodologie predittive del fabbisogno sanitario, per il quale le regole di protezione dei dati potranno rappresentare un prezioso presupposto di efficacia.

Anche questi esempi dimostrano, dunque, come, sulla sinergia tra innovazione, *governance* sanitaria e protezione dei dati, si giocherà una sfida sempre più determinante per le nostre società, che dobbiamo impegnarci a vincere all'insegna, ancora una volta, della centralità della persona e della sua dignità, quei vincoli che – spiegò Aldo Moro in Assemblea costituente – neppure l'interesse collettivo alla sanità pubblica può superare.

PRESIDENTE. Grazie, presidente. Do la parola all'onorevole De Toma, che intende porre un quesito.

MASSIMILIANO DE TOMA (MISTO). Grazie, presidente, grazie, presidente Soro. Devo dire che questa audizione è un'audizione per noi centrale, perché tutte le audizioni che abbiamo svolto precedentemente portavano poi a dover analizzare quelli che sono i problemi sorti fra regioni e soprattutto anche fra altre associazioni, e il tutto confluiva sui dati, dati che effettivamente creano delle problematiche, soprattutto per l'importanza, come ha detto lei, della protezione dei dati stessi dagli attacchi informatici. Questo, ovviamente, lo abbiamo potuto vedere anche su altri aspetti, oltre che su quello sanitario, ma è certo che la situazione sanitaria del momento, purtroppo, ha fatto sì che ci fosse un'accelerazione per la necessità, in questo caso con riferimento all'*app* Immuni, di un controllo e di una verifica sui pazienti e i cittadini, in considerazione della situazione grave del momento. Noi, come Commissione bicamerale per la semplificazione, siamo stati in un certo senso precursori, perché avevamo iniziato molto prima, proprio perché avevamo individuato, attraverso il fascicolo sanitario e tutto quello che ne consegue, la possibilità di ottimizzare il percorso, attraverso uno strumento, quale un'*app* o una tessera sanitaria, che sia comunque atto a semplificare la quotidianità del cittadino.

Le pongo tre domande. Il suo intervento è stato molto esaustivo, e quindi qualcosa può anche ripetersi, magari potremmo verificarlo insieme. Le pongo la prima domanda: il cittadino ha diritto alla portabilità dei dati ovvero, nello specifico, il cittadino può utilizzare i propri dati consentendo l'accesso al suo interlocutore di turno ? La domanda in realtà nasce perché, in base alle norme sulla *privacy*, il cittadino ha diritto di chiedere a chi ha raccolto i dati personali di cancellarli oppure di averli in formato portabile e, quindi, trasferibili ad altro *database*. La seconda domanda concerne il consenso informato affinché i dati sanitari raccolti siano utilizzati a fini di ricerca Se vengono raccolti dei dati, per esempio quelli dell'esame del sangue, que-

sti possono essere aggregati, resi anonimi e utilizzati a scopo di ricerca, per esempio generando pubblicazioni scientifiche, senza che il paziente lo sappia ? L'ultima domanda: si sta facendo qualcosa per aumentare il numero di *app* che possano surrogare l'intervento umano nella raccolta dei dati degli utenti, ovviamente con la necessaria protezione certificata delle soluzioni offerte ?

Concludo riprendendo quello che lei ha riferito circa il cosiddetto « decreto rilancio », che andremo a discutere e a esaminare nei prossimi giorni, che è assolutamente importante per quanto concerne il fascicolo sanitario e quello che ne consegue. Al di là dell'attività parlamentare che ognuno di noi svolge nelle proprie Commissioni di appartenenza, in questa Commissione bicamerale penso che sia l'aspetto centrale, proprio perché termineremo questo percorso, come ha annunciato il presidente, entro la fine di luglio, e proprio per questo vorremmo trovarci pronti, ma soprattutto far trovare pronti i cittadini, a un'ottimizzazione generale di costi e di informazioni.

PRESIDENTE. Vorrei aggiungere solo un'altra cosa. Vista la situazione nella quale ci stiamo muovendo, chiederei al presidente Soro, qualora ci fossero domande da parte di colleghi che seguiranno successivamente questa nostra audizione, la possibilità di avere delle risposte. Siccome c'era molta attenzione a questa audizione, sono sicuro che magari nelle prossime ore potrebbero esserci dei colleghi che la vedranno in differita e potranno porre alcune domande, per cui chiedo la disponibilità del presidente a fornire risposte scritte a eventuali domande che fossero formulate successivamente per iscritto.

Intendo, inoltre, svolgere una riflessione e porre una domanda. Lei oggi, e la ringrazio, ha fatto una relazione completa, esaustiva e anche innovativa, se posso dire, della modalità con la quale la giurisprudenza sulla *privacy* fin qui aveva guardato al modello sanitario. È giusto, perché in momenti come questi ognuno deve assumere dei passi ulteriori. Ritengo tuttavia – valeva prima e vale adesso – che dentro al sistema, che io mi auguro sia digitale prima possibile, della sanità debba trovarsi quello a cui noi daremo possibilità di accesso, ed è quello che lei prima ci diceva. Alcune modalità sono state semplificate; l'autorizzazione ora avviene soltanto nel momento iniziale, non c'è più bisogno di alcuni passaggi. Credo, nell'interesse delle cose che lei ha detto e dei cittadini, che il tema cruciale non sia l'istituzione del fascicolo, che, anzi, va accelerata. Lei giustamente ha parlato di modalità da remoto della medicina che sono già possibili, ma che non sono completamente utilizzate. Penso, per esempio, alla telemedicina o ad altri sistemi. Il punto centrale, dal mio punto di vista, resta la parcellizzazione del sistema, cui si è tentato di porre rimedio attraverso il fascicolo centrale, quindi accorpando i ventuno fascicoli (che poi non sono ventuno, ma in realtà sono molti di meno quelli che già funzionano). Superata questa fase, bisogna trovare il sistema centrale di difesa per eventuali aggressioni cibernetiche, se così posso definirle, che vanno alla ricerca non tanto dei dati, ma dell'utilizzo dei dati sensibili. Nelle varie Commissioni competenti c'è stato e c'è un dibattito sulla *cyber security* di un certo livello; il nostro Paese si sta attrezzando ancora di più e meglio. La domanda è cosa serve perché questi dati siano sicuri dal punto di vista della protezione dei dati personali, utilizzabili ai fini medici della persona, e non diventino invece una massa di informazioni enorme il cui utilizzo sia più economico che scientifico e medico sulla persona. Il rischio oggettivo, infatti, è che questa massa di dati, anziché servire a curare le persone, serva poi in altre situazioni per fare, se posso dirlo volgarmente, cassa, cosa che tutti noi vorremmo evitare, anzi vorremmo avere una sanità capace di lavorare al meglio nell'interesse dei cittadini.

ANTONELLO SORO, *presidente dell'Autorità Garante per la protezione dei dati personali*. Grazie, presidente. Naturalmente c'è tutta la mia disponibilità per un'ulteriore interlocuzione nelle forme che lei riterrà.

Inizierei dalla prima considerazione fatta dall'onorevole De Toma. Nella medicina,

nell'ambito della salute, il rischio informatico è particolarmente rilevante perché si traduce in rischio clinico. Questa considerazione spesso viene sottovalutata nel dibattito pubblico, in cui si parla di *privacy* qualche volta con un'approssimazione tendenzialmente non amichevole. Nella dimensione digitale la *privacy* diventa protezione del dato. La declinazione di *privacy* dentro la dimensione digitale è protezione del dato, e la protezione del dato equivale alla protezione delle nostre persone in quella dimensione. Quindi, se questa diventa la consapevolezza, penso che nell'approccio alla vita digitale, con il desiderio di svilupparla quanto più è possibile, l'esigenza di metterla in sicurezza, dotandola di tutti i presidi che garantiscano le tutele dei cittadini e delle persone, così come abbiamo preteso nella storia dell'umanità di averle garantite nella dimensione fisica, sia un punto assolutamente decisivo.

La seconda considerazione riguarda la novità, effettivamente molto importante, che si verifica oggi con il cosiddetto « decreto rilancio », che mette fine al processo di allestimento del fascicolo sanitario elettronico attraverso il consenso, per armonizzare il fascicolo sanitario elettronico nella sua alimentazione a quanto il nuovo regolamento europeo ha stabilito, decidendo che i dati sulla salute raccolti per finalità sanitarie da parte del medico e della struttura medica non avessero più necessità del consenso. Il consenso diventava, con riferimento al generico trattamento dei dati, una formalità che non aveva più nessuna ragione di obiettivo di tutela, ma diventava burocrazia. Quando uno va dal medico e racconta la sua vita e gli offre il suo braccio per fare un prelievo di sangue, in quel momento c'è tutto il consenso possibile; quindi, il regolamento ha attualizzato questa previsione e noi abbiamo segnalato al Parlamento l'utilità di allineare l'alimentazione del fascicolo sanitario elettronico in questa direzione. Naturalmente, da questo deriva una grande responsabilità, in primo luogo quella di controllare l'architettura. Lei, presidente, faceva riferimento a questo obiettivo, ma l'obiettivo di superare la frammentazione regionale significa anche superare le diverse forme attraverso le quali si garantisce l'architettura.

L'architettura nella quale si deposita il fascicolo e si alimenta il fascicolo sanitario elettronico deve essere una, deve avere il massimo della garanzia, e il nostro Paese deve farsi carico, deve avere l'obiettivo di creare una nuova, grande infrastruttura per la conservazione dei dati più delicati. Non possiamo mettere sullo stesso piano un qualunque *server* nel quale affluiscono i dati della vita di tutti gli italiani, anche i più banali, e la scatola nella quale stiamo immettendo i dati più rilevanti per il cittadino, per lo Stato. Naturalmente, non saranno solo quelli relativi alla salute i dati più importanti, ma sono fra quelli più importanti. L'idea di avere un'infrastruttura totalmente italiana, totalmente garantita dalla stessa regola, dalla stessa robustezza del presidio della sicurezza cibernetica, deve essere, a mio avviso, un grande obiettivo del nostro Paese.

In questo contesto rientra anche il tema di cui si è discusso molto in queste settimane, quello della sicurezza o meno dell'*app* Immuni. A me ha fatto molto piacere vedere un grande interesse da ogni parte del panorama politico e informativo sull'*app* Immuni. Vorrei, però, dire che c'è uno sbilanciamento, c'è una sproporzione rispetto all'interesse che viene posto abitualmente per la sicurezza di dati più importanti di quelli che l'*app* Immuni raccoglie. Se l'*app* Immuni circola dentro l'infrastruttura nella quale circolerà il fascicolo sanitario elettronico, allora il tema è mettere in grande sicurezza tutto il sistema che raccoglie dati sulla salute. In questo senso, ritengo che l'esperienza dei dibattiti di queste settimane possa essere il presupposto per un passo in avanti nella direzione di una dimensione digitale più sicura per gli italiani.

PRESIDENTE. Grazie, presidente, non solo per la relazione, ma anche per le risposte che ci ha dato. Sono sicuro che questo punto di centralità che lei ci ha indicato sull'importanza di un sistema nazionale unico, sicuro, verso il quale far confluire i dati, sia condiviso – lo posso anticipare per quello che è stato il dibattito

di questa Commissione – e credo che se ne terrà conto nella nostra relazione. Oggettivamente trattare i dati sanitari come se fossero dei normali dati e poterli inserire in qualsiasi *server* diventerebbe il punto di non ritorno anche per il Paese e saremmo in balia dei quattro venti, se non peggio, guardando alle politiche internazionali, ai movimenti che ci sono e agli appetiti verso i dati. La ringrazio nuovamente, presidente, anche per la disponibilità a rispondere a eventuali ulteriori domande.

Dichiaro conclusa l'audizione.

La seduta termina alle 11.15.

Licenziato per la stampa
il 23 giugno 2020

STABILIMENTI TIPOGRAFICI CARLO COLOMBO

18STC0103730