



15/09/2022 11:16  
Sito Web

key4biz

## Sanità digitale, Alessandro Del Ninno (LUISS) 'Garante Privacy costretto a bocciare i decreti sulla banca dati sanitaria e sul fascicolo sanitario elettronico'

LINK: <https://www.key4biz.it/sanita-digitale-alessandro-del-ninno-luiss-garante-privacy-costretto-a-bocciare-i-decreti-sulla-banca-dati-sanitaria-...>



FONDAMENTI DI DIRITTO  
PRIVACY COMPARATO | EDIZIONE 3  
NORME INTERNAZIONALI A CONFRONTO

15%  
sconto  
CODICE  
LPAKEY1

DAL  
19  
OTTOBRE

Sanità digitale, Alessandro Del Ninno (LUISS) 'Garante Privacy costretto a bocciare i decreti sulla banca dati sanitaria e sul fascicolo sanitario elettronico' a cura di Paolo Anastasio | 15 Settembre 2022, ore 11:10 Internet Il professor Alessandro Del Ninno analizza la doppia bocciatura dei decreti su banca dati sanitario e fascicolo sanitario elettronico da parte del Garante Privacy. 'In sostanza bocciate logica e sostanza'. Il Garante Privacy ha recentemente bocciato i decreti sulla la banca dati Ecosistema Dati Sanitari (EDS) e quello sul Fascicolo sanitario elettronico (Fse), dando parere negativo al Ministero della salute e al Ministero per l'innovazione tecnologica e la transizione digitale sullo schema di decreto che prevede la realizzazione della nuova banca dati denominata Ecosistema Dati Sanitari (EDS), prevista dalla riforma del Fascicolo sanitario elettronico. Il Garante ha chiesto anche di correggere un secondo

schema di decreto, per favorire e migliorare l'implementazione a livello nazionale del Fascicolo sanitario elettronico (FSE). Abbiamo chiesto un parere su questa doppia bocciatura al Prof. Avv. Alessandro del Ninno, Partner IT di Tonucci & Partners - docente di Informatica Giuridica alla LUISS Guido Carli di Roma. Key4biz. Perché questa doppia bocciatura del Garante in tema di sanità digitale? Alessandro del Ninno. Il Garante boccia la logica e la metodologia adottata: in sostanza, visto che l'EDS si alimenta con i dati del FSE, non si comprende come abbiano potuto le autorità competenti scrivere il decreto sull'Ecosistema dei Dati Sanitari senza aver prima definito i decreti che disegnano il sistema del riformato Fascicolo Sanitario Elettronico e senza aver compiutamente attuato le indicazioni di conformità che il Garante ha fornito sul FSE con i suoi pareri fin dal 2014, tanto che il Garante dichiara per tali motivi la sua

impossibilità a valutare e rendere il Parere su EDS. Oltretutto, per il Garante l'EDS come allo stato delineato dal decreto - è una "scatola vuota", poiché rinvia a successivi decreti la definizione di molti aspetti essenziali per la sua regolamentazione (ad esempio: chi può accedere ai dati o quale è il contenuto dei dati). Key4biz. C'è dell'altro che il Garante contesta? Alessandro del Ninno. Per il Garante, poi, i due schemi di decreto su EDS e FSE sono viziati da estrema genericità e indeterminazione quanto ad aspetti fondamentali sulla protezione dei dati personali. Faccio solo un esempio, per evidenziare quanta incompetenza e quanto scadimento connotano ormai la redazione delle norme da parte del nostro Legislatore: il Garante afferma che l'Informativa sul trattamento dei dati personali allegata ad entrambi gli schemi di decreto su EDS e FSE "è sostanzialmente priva di tutti gli elementi richiesti

dagli artt. 13 e 14 del Regolamento 679/2016" e va "integralmente riformulata". Ma ci rendiamo conto?? Chi ha scritto i decreti neanche si è andato a leggere gli articoli 13 e 14 del GDPR che elencano gli elementi fondamentali dell'Informativa.... Key4biz.

Ci sono altri elementi rivedibili? Alessandro del Ninno. Il Garante bocchia, poi, la visione generale e la mancanza di coordinamento tra i due schemi di decreto su EDS e FSE e i diversi altri atti normativi che stanno introducendo e rafforzando - anche alla luce degli obblighi di cui al PNRR - strumenti e servizi di Sanità Digitale nel nostro paese. È ovvio che tutte le regole - sia legali che tecnico-organizzative (si pensi per queste ultime alla interconnessione di vari sistemi e database del SSN) - devono essere coerenti tra loro. E proprio tale mancanza di coerenza e coordinamento il Garante lamenta come vulnus di carattere generale di entrambi i due decreti su EDS e FSE. Key4biz. E dal punto di vista della data protection? Alessandro del Ninno. Il Garante si esprime con toni particolarmente severi sulle carenze data protection degli schemi di decreto, carenze che definisce "strutturali, sostanziali e

considerevoli..." presentando "numerosi profili di violazione della disciplina in materia di protezione dei dati personali". Tanto che sostanzialmente ne propone una quasi integrale riformulazione. Vedremo anche che dirà anche l'Agenzia per la cybersicurezza nazionale, che pure deve rilasciare - per i profili di competenza - il suo parere. Key4biz. Quanto alla mancanza di coordinamento con altre normative che il Garante segnala, con quali ulteriori regole di costruzione di un sistema nazionale di Sanità Digitale si dovrebbero coordinare i due schemi di decreto su EDS e FSE? Alessandro del Ninno. L'ultimo triennio è stato caratterizzato dalla forte accelerazione e sviluppo di norme che regolano gli strumenti di sanità digitale nel nostro Paese. Di qui l'esigenza primaria di un coordinamento normativo che difatti il Garante richiama come necessità ineludibile. Le norme attuative su EDS e FSE si dovrebbero coordinare, ad esempio, con il decreto previsto dal novellato art. 2 sexies, comma 1-bis, del Codice della privacy, in cui saranno disciplinati i dati personali relativi alla salute, privati degli elementi identificativi diretti, che potranno essere trattati, nel

rispetto delle finalità istituzionali, dal Ministero della salute, dall'Istituto superiore di sanità (ISS), dall'Agenzia nazionale per i servizi sanitari regionali (AGENAS), dall'Agenzia italiana del farmaco (AIFA), dall'Istituto nazionale per la promozione della salute delle popolazioni migranti e per il contrasto delle malattie della povertà (INMP), relativamente ai propri assistiti, dalle regioni/province autonome anche mediante l'interconnessione a livello nazionale dei sistemi informativi su base individuale del Servizio sanitario nazionale (SSN), ivi incluso il FSE. I decreti su EDS e FSE dovrebbero poi coordinarsi anche con le nuove norme sulla cosiddetta "medicina predittiva" derivanti dalla riforma del decreto-legge 34/2020. O, infine, con il futuro Regolamento UE sullo Spazio Europeo dei Dati Sanitari, di recente approvato. Il Garante rileva che persino le recenti "Linee guida per l'attuazione del FSE" (pubblicate nella gazzetta dell'11 Luglio 2022) che indicano le regole tecniche sono state adottate in maniera "scoordinata" e con modalità difformi rispetto a quanto previsto dall'articolo 12, comma 15-bis, d.l. n. 179/2012, specie da un punto di vista sostanziale,

in quanto intervengono su aspetti diversi da quelli indicati del decreto che nel 2012 ha introdotto il FSE.

Key4biz. C'è un modello europeo da seguire per non incorrere in ulteriori bocciature da parte del Garante Privacy? Alessandro del Ninno. Certamente, è lo stesso Garante a ricordarlo: la recente proposta di Regolamento UE sullo Spazio Europeo dei Dati Sanitari (uno degli 11 "Spazi Europei" settoriali che rivoluzioneranno lo scambio dei dati nei mercati digitali, sotto l'egida dell'importante Regolamento 868/2022 sulle Governance europea dei dati il Data Governance Act che è definitivo e sarà applicabile dal prossimo 24 Settembre 2023) è un modello di riferimento, soprattutto se la Commissione recepirà i suggerimenti del Comitato europeo per la protezione dei dati personali finalizzati al raggiungimento di un equilibrio tra l'agevolazione della disponibilità di dati sanitari elettronici e l'impatto sui diritti e la libertà dei cittadini. Ancora più precisamente, il modello di riferimento può essere la costruzione teorica del sistema che i Garanti UE fanno nel loro recente Parere 3/2022 sulla proposta di Regolamento UE sullo Spazio europeo dei

Dati Sanitari. Key4biz. Cosa è la banca dati dell'Ecosistema Dati Sanitari? Alessandro del Ninno. In sostanza l'Ecosistema Dati Sanitari (EDS) è una vasta banca dati pubblica che dovrebbe garantire il coordinamento informatico e assicurare servizi sanitari digitali omogenei sul territorio nazionale per il perseguimento delle finalità del Fascicolo Sanitario elettronico (a cui è strettamente connessa). La banca dati dell'EDS si alimenterebbe con i dati trasmessi dalle strutture sanitarie e socio-sanitarie, dagli enti del Servizio sanitario nazionale e da quelli resi disponibili tramite il sistema Tessera Sanitaria; inoltre, si alimenterebbe mediante duplicazione di dati e documenti sanitari già presenti nel FSE (e questo aspetto è severamente criticato dal Garante privacy, unitamente alla mancanza di anonimato per i cittadini-pazienti censiti). Così costruito, l'EDS diventerebbe la più grande banca dati centralizzata sulla Salute del nostro Paese, contenente fra l'altro tutte le prestazioni sanitarie erogate sul territorio nazionale. Il Ministero della salute sarebbe il Titolare del trattamento dei dati contenuti nell'EDS, mentre la gestione operativa

sarebbe delegata all'AGENAS (Agenzia Nazionale per i Servizi Sanitari) in qualità di Responsabile del trattamento ai sensi dell'art. 28 GDPR. Quanto alla funzione dell'EDS, tale repository centrale acquisirebbe e tratterebbe i dati sanitari e non solo mediante particolari elaborazioni (anche attraverso logiche algoritmiche) per poi offrire specifici servizi agli esercenti le professioni sanitarie, al Ministero della salute, alle regioni/province autonome e allo stesso cittadino. Key4biz. Cosa è il Fascicolo sanitario elettronico? Alessandro del Ninno. Intanto il Fascicolo Sanitario Elettronico, nei suoi rapporti con l'EDS, può considerarsi la sua base logico-giuridica visto che l'Ecosistema si alimenta proprio con i dati del FSE. Il FSE è uno strumento per reperire parte dei dati e dei documenti relativi alla storia sanitaria di un individuo con lo scopo di fornire uno scenario generale della sua salute ai professionisti sanitari che lo prendono in cura, che non sono comunque allo stato-obbligati a consultarlo né ad alimentarlo. Più precisamente, e da un punto di vista più giuridico il d.l. 179/2012 lo definisce come l'insieme dei dati e documenti digitali di tipo

sanitario e socio-sanitario generati da eventi clinici presenti e trascorsi, riguardanti l'assistito, riferiti anche alle prestazioni erogate al di fuori del Servizio sanitario nazionale. E se c'è lo specifico consenso dell'interessato, il FSE può anche essere utilizzato per finalità di cura, prevenzione e profilassi internazionale. Infine, e di riflesso, il FSE è in sostanza un sistema di raccolta di informazioni sulle prestazioni sanitarie rese all'assistito al fine di delineare un preciso profilo sanitario dello stesso: in questo, il FSE non va confuso con la cartella sanitaria (che è un atto pubblico) e non certifica la salute di un individuo, limitandosi a fornire informazioni sanitarie (anche incomplete, tra l'altro) che possono agevolare il percorso di cura. Key4biz. A proposito di app medicali, secondo un recente studio due italiani su tre hanno provato almeno una app medicale. Ma i rischi privacy dal loro utilizzo paiono evidenti. Ma lei cosa ne pensa delle app medicali? Alessandro del Ninno. L'universo delle app o delle funzioni di monitoraggio dello stato sanitario oramai standard nei nostri dispositivi è molto variegato. Funzioni come l'App "Salute" di Apple sono ormai integrate in telefonini

e smart watch. Si va dalle funzioni contapassi a quelle che misurano battito cardiaco, pressione e livelli di ossigeno nel sangue. Fino ad app più complesse, come quelle associate a dispositivi medici (ad esempio: suole smart per anziani che rilevano con l'app correlata la modalità di camminata per trarne dati - anche predittivi - sullo stato di osteoporosi ossea). Ve ne sono alcune di straordinaria utilità per il monitoraggio della salute (come quelle che consentono un contatto continuo con il medico di base); altre facilitano l'accesso ai servizi sanitari (penso alle app con cui prenotare on line prestazioni medico-sanitarie). È ovvio che il rischio è però quello della mancata consapevolezza su come queste app trattano i nostri dati sanitari. E questa consapevolezza manca quasi sempre (come anche le indagini del Garante sulle app medico-sanitarie hanno rilevato) a causa o di informative mal redatte o della mancata attitudine di chi le scarica e le utilizza a verificare - prima di metterle in uso - che fine fanno informazioni così particolari - come quelle sanitarie - che consentono la creazione di profili socio-sanitari molto appetibili, ad esempio, per le assicurazioni. Faccio un

esempio: andando a leggermi le condizioni generali e le informative di una app di fitness che volevo utilizzare per creare un diario di allenamento, scoprii che ero obbligato a consentire il trasferimento dei miei dati sanitari in USA e che il fornitore avrebbe potuto venderli a terzi. Ovviamente, quella app la ho segnalata al Garante, ma chissà quanti altri utenti che la hanno utilizzata sono consapevoli di quanto ho raccontato..... Key4biz. Sono affidabili? Alessandro del Ninno. Dipende se Lei riferisce l'affidabilità all'aspetto sanitario o alla tutela dei dati. Sul primo aspetto, è sempre assolutamente sconsigliabile - soprattutto per la propria salute - affidarsi al fai-da-te. Quindi il grado di affidabilità per gli aspetti sanitari è ovviamente prossimo allo zero se non ci si rivolge a un professionista medico-sanitario o non si utilizzano certe app sotto controllo e con la consulenza di un professionista. Quanto agli aspetti data protection, ho rilevato nelle mie analisi e per le mie esperienze professionali nel settore poca affidabilità circa il livello di rispetto dei diritti e delle libertà fondamentali degli utenti e dei loro dati personali. Ma non possiamo generalizzare: esistono anche eccellenze e app

sanitarie molto affidabili. Tra l'altro, esistono Linee Guida e Protocolli pubblici che valutano l'affidabilità delle app sanitarie disponibili sugli store digitali. Key4biz. Come vengono protetti i dati sensibili raccolti? Alessandro del Ninno. Il problema, per molte app medico-sanitarie, è capire se i dati sanitari raccolti vengono efficacemente protetti... Una misura per certi versi standard è la crittografia, ma quanti la impiegano? Da un punto di vista giuridico, la pseudonimizzazione o l'anonimizzazione sono misure tecnico-organizzative che subito vengono in considerazione quando si parla di protezione dei dati di particolare natura, come i dati sanitari. Key4biz. Esiste una regolamentazione di queste app medicali, un registro che le raccoglie, oppure ci troviamo un far west normativo? Ricordo i diversi interventi del Garante rispetto al fiorire di app analoghe ad Immuni durante la pandemia. Alessandro del Ninno. Intanto va ricordato che l'articolo 9, comma 1, del Regolamento generale UE sulla protezione dei dati personali 679/2016 prevede un divieto generale di trattare le "categorie particolari di dati", tra cui rientrano quelli sulla salute,

ad eccezione di alcuni casi esplicitamente indicati ad esempio se l'utente ha fornito un consenso informato, consapevole e specifico per ogni finalità o se il trattamento persegue motivi di interesse pubblico o finalità di medicina preventiva, diagnosi, assistenza o terapia sanitaria e solo in seguito all'adozione di particolari garanzie. Alcune regole sulle app medico-sanitarie possono ritrovarsi nell'importante Provvedimento n. 55 del 7 marzo 2019, con cui il nostro Garante ha fornito chiarimenti in relazione al trattamento dei dati personali in ambito sanitario. Key4biz. Quali rischi dall'uso distorto di questi dati sulla salute? Alessandro del Ninno. Intanto, occorre ricordare che andiamo verso una Sanità digitale dove sempre più diffuso sarà l'impiego di soluzioni algoritmiche a scopi predittivi (anche per prevenire pandemie - per quanto possibile o a scopi di tracciamento) e di Intelligenza Artificiale nell'ambito di sistemi informativi medico-sanitari sempre più interconnessi. E questo è già di per sé una sorta di "rischio sistemico". Si pensi alle riforme della disciplina sulla realizzazione del modello predittivo del fabbisogno di salute della popolazione assistita (art.

7, comma 1-bis, d.l. n. 34 del 2020 che ha introdotto la cosiddetta "medicina predittiva") e di quella sull'interconnessione a livello nazionale dei sistemi informativi su base individuale del SSN (art. 2 sexies, comma 1-bis, del Codice della privacy come recentemente novellato). A maggior ragione, l'enorme disponibilità di dati in assenza di tutte le misure (preventive) di giusto assessment dei rischi, rendono probabile il verificarsi di eventi quali: la re-identificazione degli interessati a cui si riferiscono i dati sanitari non pseudonimizzati o non correttamente anonimizzati, accessi abusivi e illeciti; utilizzo dei dati per finalità non compatibili; discriminazione algoritmica e uso distorto di nuove tecnologie basate su logiche algoritmiche e strumenti di intelligenza artificiale; trattamenti automatizzati che possono avere ricadute sul singolo interessato, etc Sanità digitale L'autore Paolo Anastasio Condividi: