INFORMATICA GIURIDICA
Collana diretta da Giovanni Ziccardi e Pierluigi Perri

9

Massimo Farina

Il cloud computing in ambito sanitario tra security e privacy

Prefazione di Antonello Soro

Giuffrè Francis Lefebvre

Sezione non inclusa

PREFAZIONE

Questo importante saggio affronta, con grande rigore, il tema del rapporto tra sanità e digitalizzazione, che rappresenta una delle sfide principali per la garanzia dell'unico diritto che la nostra Costituzione espressamente qualifica, ad un tempo, come diritto fondamentale e interesse della collettività. E per il quale sancisce una riserva di legge rafforzata, prevedendo che nessun trattamento sanitario, ancorché legislativamente disposto, possa violare "i limiti imposti dal rispetto della persona umana". Formula, questa, che Costantino Mortati riconosceva come complementare alla tutela della dignità, sancita da quell'art. 2 cui Aldo Moro attribuiva la funzione di difesa della persona da ogni strumentalizzazione per fini che la trascendano. Ed è significativo che soltanto la Carta di Nizza (che non a caso si apre con l'enunciazione della dignità quale presupposto di ogni libertà e diritto fondamentale) preveda un livello di tutela analogo del diritto alla salute, codificando nel consenso informato l'essenziale presidio della libertà di autodeterminazione terapeutica. E questo, con un singolare parallelismo rispetto al consenso informato al trattamento dei dati personali, su cui si incentra la libertà di autodeterminazione informativa, ovvero il nuovo diritto di libertà sancito dalla stessa Carta di Nizza, autonomamente rispetto al tradizionale diritto alla riservatezza.

Questo parallelismo dimostra come tanto l'autodeterminazione informativa quanto l'autodeterminazione terapeutica siano due aspetti essenziali della libertà e della dignità della persona oggi, entrambi meritevoli di una tutela tanto intensa quanto dinamica così da potersi adeguare alla rapidità propria dell'evoluzione tecnologica e scientifica, con cui questi diritti costantemente si rapportano. L'equilibrio tra i due è garanzia di qualità ed efficienza delle cure e del sistema sanitario cui il paziente si affida; tanto più in un contesto di progressiva digitalizzazione dei percorsi diagnostici e terapeutici.

L'applicazione della tecnologia digitale a fini di cura, di ricerca medico-scientifica e persino di governance e razionalizzazione della spesa sanitaria è infatti (e bene il libro lo sottolinea), un fattore

essenziale di sviluppo, crescita e benessere per il Paese e per i cittadini, oltre che di miglioramento dell'efficienza delle prestazioni. Quello della digitalizzazione della sanità è, dunque, un processo che va promosso ma che va anche governato con attenzione, in quanto coinvolge categorie di dati personali (tra le più delicate e, per questo, meritevoli di quella tutela rafforzata che il nuovo quadro giuridico europeo per la protezione dati — come già la direttiva madre — loro assegna.

Ed è significativo che per i dati sulla salute il regolamento europeo sulla protezione dati, pur promuovendo, condivisibilmente, con misure di favore la ricerca scientifica, sancisca non solo una tutela rafforzata ma legittimi i singoli ordinamenti, con una clausola di flessibilità, ad introdurre ulteriori garanzie. Valorizzate, peraltro, dal legislatore nazionale, che con il D.Lgs. 101/2018, (oltre ad escludere la necessità del consenso al trattamento dei dati per fini terapeutici salvo ipotesi specifiche), ha però previsto sul punto l'obbligo di conformità del trattamento alle misure di garanzia sancite dal Garante, in particolare per elevarne gli standard di sicurezza.

I dati sulla salute, se illecitamente trattati o — come avvenuto più volte — addirittura "rubati", sono infatti suscettibili di esporre l'interessato a forme di stigmatizzazione sociale o discriminazione rese possibili, appunto, soltanto dalla conoscenza di aspetti così intimi quali quelli "idonei a rivelare lo stato di salute dell'interessato".

Per questo, nel processo di digitalizzazione della sanità la frammentazione (anche a livello di soggetti coinvolti e delle relative responsabilità sul trattamento dei dati), l'assenza di un piano organico di sicurezza e la disomogeneità che hanno caratterizzato, purtroppo, l'informatizzazione della p.a. nel nostro Paese (con gravi rischi anche in termini di cybersecurity), sono ancora più pericolose che in ogni altro settore. Perché la perdita, la sottrazione, l'alterazione, l'abuso di un dato sanitario rende vulnerabili banche dati essenziali e, insieme, viola quanto di più intimo e privato vi è nella persona; ne tocca la dignità.

Ma soprattutto, la vulnerabilità del dato sulla salute e, quindi, la suscettibilità di alterazione o modificazione, rischia — come abbiamo sottolineato anche rispetto al FSE — di determinare errori diagnostici o terapeutici, con conseguenze anche letali. La carente sicurezza dei dati e dei sistemi che li ospitano può rappresentare, in altri termini, una causa di malasanità. E, per converso, la protezione dei dati personali e dei sistemi (informativi, biomedicali) è un fattore determinante di efficienza sanitaria. Si pensi, ad esempio, al noto caso di cronaca che ha interessato un ospedale statunitense, in cui un attacco hacker al sistema

informatico ha bloccato per lungo tempo l'erogazione dei servizi e l'analisi dei dati sanitari dei pazienti.

Sotto questo profilo, anche (e forse soprattutto) da noi la strada da fare è ancora tanta: recenti ricerche hanno indicato, infatti, il settore sanitario come uno di quelli esposti ai maggiori rischi in termini di *cybersecurity* perché carente di un piano organico di sicurezza e protezione, oltre che di risorse necessarie per investimenti sulle infrastrutture informative.

Eppure, proprio questo dovrebbe essere, invece, il settore su cui investire di più in termini di sicurezza e resilienza, così da accompagnare l'innovazione tecnologica alle garanzie, soprattutto in un contesto di sempre maggiore utilizzo del *cloud computing* (che dovrebbe auspicabilmente portare alla realizzazione di un cloud europeo) e della *big data analytics* a fini di ricerca scientifica o più propriamente di cura.

Al riguardo, in particolare, va ricordato come la protezione dei dati sia funzionale anche alla stessa correttezza del processo analitico fondato su *big data*, ove le scelte algoritmiche sono rese possibile dall'autoapprendimento di cui è capace la macchina a partire dai dati immessi, di cui va quindi garantita la qualità.

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 la conseguente diagnosi ad essere sbagliata, con effetti potenzialmente anche fatali per il paziente. La protezione dei dati, dunque, tutt'altro che un ostacolo, è invece un presupposto di efficacia della *big data analytics*, soprattutto in un settore così delicato come quello sanitario.

Sotto questo profilo, il nuovo quadro giuridico europeo offre importanti garanzie, esigendo in particolare trasparenza e contestabilità del processo algoritmico, cautele specifiche per la delocalizzazione del trattamento e in senso più lato un approccio generale fondato sulla prevenzione del rischio, con la previsione di misure precauzionali e l'adozione di una strategia complessiva volta alla protezione dei dati e alla responsabilizzazione dei protagonisti del trattamento.

Il libro offre una panoramica quantomai ampia e articolata su questi nuovi scenari della società digitale, ben sottolineando come gli istituti giuridici tradizionali — e gli stessi confini dell'autonomia negoziale — debbano necessariamente rimodellarsi in funzione delle implicazioni dirompenti del digitale sulla vita privata e pubblica. Entra così in gioco, rispetto ai contratti informatici e in particolare del *cloud*

computing, non solo il tema dell'articolazione dei rapporti tra titolare e responsabile in un contesto così complesso, ma anche quello della locazione dello spazio web e della centralità dei dati come elemento di classificazione negoziale.

Gli stessi istituti a tutela del contraente debole e gli strumenti di eterointegrazione del contratto si ridefiniscono, con implicazioni inattese, a fronte dell'impatto prodotto dalla digitalizzazione sull'autonomia negoziale, tanto più ove siano in gioco i diritti fondamentali alla salute e alla protezione dei dati.

Sulla sinergia tra salute, innovazione e protezione dati si giocherà, dunque, una sfida sempre più determinante per le nostre società, che dobbiamo impegnarci a vincere nel segno, ancora una volta, della centralità della persona e della sua dignità. Ripensare al diritto in tal senso, come fa questo saggio, ne è sicuramente il presupposto ineludibile.

ANTONELLO SORO
Presidente dell'Autorità Garante per la protezione dei dati personali

Capitolo I
DALL'*E-GOVERNMENT* (1) ALL'*E-HEALTH*

1. *I sistemi informativi sanitari: aspetti generali*

I sistemi informativi sanitari (2), appositamente creati per la gestione dei flussi di dati prodotti dal sistema sanitario nel suo insieme,

---

(1) Per un inquadramento del "sistema" italiano dell'e-Government, si v., F. Merloni, *Introduzione all'eGovernment* (Torino: Giappichelli, 2005), nonchè già G. Vesperini, *L'e-Government* (Milano: Giuffrè, 2004); il Codice dell'amministrazione digitale è stato oggetto di numerosi commenti: si veda, tra gli altri, *Codice dell'amministrazione digitale*, a cura di E. Carloni (Rimini: Maggioli Editore, 2005); *Il Codice della Pubblica Amministrazione Digitale*, a cura di G. Cassano, C. Giurdanella (Milano: Giuffrè, 2005); M. Atelli, S. Aterno, A. Cacciari, *Codice dell'amministrazione digitale. Commentario* (Roma: 2008); E. Belisario, *La nuova Pubblica Amministrazione digitale. Guida al Codice dell'Amministrazione Digitale dopo la Legge n. 69/2009* (Rimini: Maggioli, 2009), pp. 89-150.

(2) Per approfondimenti sui profili tecnici: Integrating the Healthcare Enterprise, IHE IT Infrastructure (ITI), Technical Framework, Volume 1 (ITI TF-1), Integration Profiles, Revision 9.0 — Final Text, August 31, 2012, p. 9.

consentono la comunicazione delle informazioni associate alle attività clinico-diagnostiche grazie all'utilizzo di *datasets* condivisi. In un'ottica di inquadramento generale non ci si deve, però, soffermare soltanto sulle componenti tecniche-informatiche, ma va opportunamente considerato il ruolo degli attori (persone fisiche) che, a vari livelli, partecipano alle dinamiche socio-assistenziali (3). Ciascuno dei predetti soggetti ha un ruolo nel trattamento dei dati relativi alla salute che popolano i sistemi informativi sanitari e che sono soggetti a continue minacce (come "*virus*", "*worm*", "*intruder*", "*insider*" ecc.), per le quali sorgono esigenze di protezione, che soddisfano la salvaguardia di un diritto fondamentale dei pazienti. Come si approfondirà nei successivi paragrafi, l'integrità, la riservatezza e la disponibilità dei dati personali rappresentano la base della sicurezza, che nella prassi ha condotto verso lo sviluppo di *standard* di sicurezza informatica e di specifici interventi normativi.

È, pertanto, doveroso, fin da ora, inquadrare la sicurezza dei sistemi informativi sanitari ("*security*") e la protezione dei dati personali ("*privacy*") come aspetti, seppur distinti, complementari, in quanto entrambi congiuntamente rivolti alla salvaguardia dei sistemi informatici e delle persone: le tecnologie per la sicurezza, infatti, forniscono dispositivi idonei a proteggere e tutelare le informazioni che riguardano le persone e le rassicurano al punto che esse, laddove necessario, possano liberamente esprimere il consenso. "*Security*" e "*privacy*" stanno, pertanto, entrambe alla base della progettazione nel campo ICT ("*Information Communication Technology*") e oggi questo inscindibile binomio è ancor più necessario in quanto, come si dirà meglio nel prosieguo, codificato dal legislatore europeo nel Regolamento Europeo 2016/679 (4) (di seguito semplicemente "Regolamento") con il principio "*data protection by design e by default*" (5). L'incedere comune di "*security*" e "*privacy*", però, non è sempre in discesa e senza osta-

---

(3) Tra gli altri, i pazienti e i loro familiari, i soggetti operanti all'interno delle strutture aziendali pubbliche o private (ad es. manager e personale amministrativo, operatori sanitari e para-sanitari, ricercatori ecc.).

(4) Regolamento 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento Generale sulla Protezione dei Dati, in forma abbreviata anche semplicemente RGPD oppure con l'acronimo inglese GDPR).

(5) F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo* (Padova: Giappichelli, 2016); l'Autore,

coli (6), in quanto, se è innegabile che la sicurezza sia funzionale alla protezione dei dati personali, tuttavia, non sempre i sistemi informativi sono messi in sicurezza in conformità alla disciplina dettata in materia di protezione dei dati personali.

1.1. *Profili di sicurezza dei sistemi informativi*

Il perseguimento dell'obbiettivo della sicurezza diventa fondamentale in una società ove la quasi totalità del patrimonio informativo è gestito tramite sistemi informatici interconnessi; in tal senso, la sicurezza deve preliminarmente declinarsi, come prevenzione di accessi non autorizzati ai sistemi informativi, così da permettere, ai soli utenti abilitati, di utilizzarli nei tempi e modi previsti. Risulta, pertanto, indispensabile la definizione di *policy* (regole e strumenti) in grado di accertare l'identità degli utenti che accedono ai sistemi informatici, di assicurare l'integrità delle informazioni che gli stessi gestiscono, nonché di garantirne il corretto funzionamento tenendo anche traccia di tutte le azioni intercorse (7).

La sicurezza informatica va progettata, prima che attuata, attraverso

---

in particolare, evidenza gli elementi di flessibilità che accompagnano l'applicazione del Regolamento.

(6) Si veda, per tutti, J. L. Fernández-Alemán et al., 'Security and privacy in electronic health records: A systematic literature review', *Journal of Biomedical Informatics*, 46 (2013), pp. 541-62, in https://www.sciencedirect.com/journal/journal-of-biomedical-informatics; B. Blobel, P. Pharow, 'Analysys and Evaluation of EHR Architecture', *Method Inf. Med.*, 2 (2009), pp. 162-169.

(7) Dal punto di vista giuridico, la "*computer security*", da raggiungere per il tramite della "*confidentiality*" (riservatezza delle informazioni), "*authentication*" (accertamento sull'identità dell'utente), "*integrity*" (integrità dei dati), "*non repudiation*" (paternità dei messaggi inviati), "*auditability*" (controllo del corretto funzionamento dei sistemi e tracciamento di tutte le azioni intercorse) e "*availability*" (disponibilità dei sistemi e dei dati ai soli utenti abilitati) è oggi ben riassunta nel principio di "*accountability*" presente nel Regolamento UE 2016/679. Nella prassi, invece, può trovarsi riscontro in alcuni criteri che sono stati definiti per la predisposizione di programmi idonei a rendere sicuri i sistemi informatici e le reti. Il primo modello al quale ci si può riferire è il cosiddetto "*confidentiality model*", al quale si riferisce, ad esempio, "*The Bell-LaPadula security model*". Un modello, quest'ultimo, elaborato agli inizi degli anni Settanta, con lo scopo di evitare il danneggiamento, deliberato o accidentale, delle informazioni da parte di individui non autorizzati a riceverle. Esso segue due principali regole: la "*Simple Security Rule*" e la "*property*". La prima limita l'accesso alle informazioni a coloro che sono dotati di specifica autorizzazione, che deve essere di livello inferiore a quella del documento di interesse; in base alla seconda, un

un'effettiva conoscenza della struttura dei sistemi di elaborazione dei dati e delle possibili problematiche sottese: ciò si traduce nella predisposizione di idonei modelli architetturali e tecnologie che rispondano ai livelli di sicurezza previsti dalle norme esistenti (8). Per garantire un elevato livello di sicurezza essenziale è la pianificazione della gestione e del controllo delle infrastrutture, con strumenti idonei, quali "*Security Information and Event Management*" (9), "*log management*" e "*change and configuration management*"; è altresì parimenti importante regolamentare forme, efficienti ed efficaci, per la valutazione dei processi ("*auditing*") e della conformità alle procedure e alle norme delineate ("*compliance*"). Il tutto, tenendo conto delle concrete modalità di trattamento delle informazioni, nello specifico contesto di riferimento (10).

---

soggetto può scrivere in un file (o, in generale, un oggetto) solo se la classificazione del suo livello di sicurezza è inferiore o uguale alla classificazione dell'oggetto.

Il secondo modello, denominato "*integrity model*", è fonte ispiratrice di altri due modelli: "*The Biba Security Model*" e "*The Clark-Wilson Security Model*". Il primo, con approccio opposto al sopraccitato "*The Bell-LaPadula security model*" si basa su due principi cardine: "*Low-Water-Mark policy*" e "*Ring policy*". Per essi, rispettivamente, da una parte un soggetto può eseguire un programma solo se il livello di integrità del programma è uguale o inferiore al livello di integrità del soggetto, dall'altra qualsiasi soggetto è autorizzato alla lettura di qualsiasi oggetto senza necessità di verificare alcun livello di integrità dell'oggetto stesso. Infine, per il modello "*The Clark-Wilson Security Model*", in dissonanza rispetto ai tutti i precedenti modelli, e quindi con approccio fortemente limitativo, un soggetto può modificare i dati solo attraverso specifici "*Trasformation processes*" ben definiti. Per ulteriori approfondimenti, WM. A. Conklin, G. White, V. Nestler, *Principles of Computer Security. CompTIA Security+TM and Beyond*, 2nd edn (McGraw-Hill Education Group, 2010) pp. 22-45.

(8) Si rimanda a quanto sarà specificato nel prosieguo a proposito del nuovo approccio sulle misure di sicurezza nel Regolamento UE 2016/679.

(9) Definisce un prodotto costituito da software e/o servizi che unisce capacità di "*Security Information Management*" (SIM) a quelle di "*Security Event Management*" (SEM). Tale denominazione è stata coniata da Amrit Williams e Mark Nicolett nel 2005, quando entrambi lavoravano per Gartner. In italiano può essere agevolmente tradotto come "Sistema di Gestione delle Informazioni e degli eventi di Sicurezza".

(10) A titolo d'esempio, pensando ad una concreta valutazione dello stato dell'arte sul quale applicare idonee misure di sicurezza, si deve considerare la distribuzione (organizzazione) dei dati (in *databases*, in *file systems*, in documenti elettronici ecc), la natura delle Reti (aziendali o pubbliche), le *policy* di l'accesso ai sistemi da parte degli utenti (identificazione e autenticazione), la conoscenza di possibili minacce e reati (essenziale per operare secondo criteri e modalità efficienti ed efficaci, che salvaguardino l'interesse del singolo e della collettività) Essenziale è, inoltre, pianificare gestione e controllo delle infrastrutture [illegible] idonei, come "*log manage-*
ment" e "*change* [illegible] forme, effi-

Capitolo II
L'EVOLUZIONE NORMATIVA DEL FASCICOLO SANITARIO ELETTRONICO

1. *La storia clinica in formato elettronico del paziente: alle origini del Fascicolo Sanitario Elettronico*

In un momento storico di grande e continua evoluzione tecnologica si tende sempre più alla mobilità nazionale ed internazionale, con conseguente necessità, tra le altre, di avere adeguati strumenti che permettano di avere sempre a disposizione la propria storia clinica, accessibile in qualsiasi momento e da qualunque luogo. In un tale scenario cambia (e deve cambiare) totalmente il rapporto tra il produttore delle informazioni (dati sanitari) e l'informazione prodotta. Quest'ultima, infatti, è, oggi più che mai, da inquadrare non più come "bene" di proprietà del medico e/o della struttura sanitaria che le ha generate, bensì come patrimonio informativo da condividere anche all'esterno del dominio aziendale del produttore con tutti i soggetti coinvolti nell'assolvimento di finalità connesse al soddisfacimento dei diritti del paziente (interessato), nonché delle esigenze dello stesso personale sanitario, para-sanitario, amministrativo. Cambia, altresì, anche il ruolo del paziente, il quale, nell'esercizio del suo ruolo di consumatore di applicazioni "sanitarie" che girano sui *mobile device*

(*laptop, tablet PC, mobile phone, smart phone, media player* etc.), riveste un ruolo sempre più centrale nella gestione della propria salute (1).

È fin dagli anni Sessanta (2) che negli Stati Uniti ci si è occupati degli aspetti architetturali ed infrastrutturali di strumenti digitali finalizzati alla raccolta di informazioni clinico-sanitarie, oggi meglio noti come Fascicoli Sanitari Elettronici (FSE).

Invero, le varie definizioni comunemente utilizzate come sinonimi di FSE non sempre sono state riferite esattamente alla medesima fattispecie (3), piuttosto a strumenti eterogenei tanto per caratteristiche tecniche ed architetturali, che per i possibili usi.

Sulla variegata panoramica sopraccitata, un valido supporto proviene dal *dossier* redatto da *International Organization for Standardization* (ISO) nel 2005 (4), nel quale è presente una rassegna dei vari tipi di piattaforme sanitarie, utilizzati dai sistemi sanitari nazionali, tra cui: "*Electronic Medical Record*" (EMR), la cui peculiarità è la raccolta "*medically focused*"; "*Electronic Patient Record*" (EPR), limitato ad una singola struttura sanitaria; "*Electronic Client Record*" (ECR), utilizzato nel contesto delle attività svolte da professionisti non medici del settore sanitario, come fisioterapisti, chiropratici o operatori sociali e, infine, il Fascicolo Sanitario Elettronico (FSE) che, nel suo significato più generico, è inquadrato come raccolta di informazioni clinico-sanitarie riferibili ad un paziente e leggibili da supporti informatici.

La panoramica del *Dossier* in esame prosegue, poi, con realtà più articolate come "*Personal Health Record*" (PHR), che si declina almeno

---

(1) La prepotente diffusione di dispositivi mobili, quali strumenti veicolatori e accumulatori di informazioni (comprese quelle sanitarie) impegna costantemente i giuristi sui profili di legittimità e sulle forme di responsabilità collegate. Si veda, tra gli altri, sul punto: H. Kharrazi et al., 'Mobile personal health records: an evaluation of features and functionality.', *International journal of medical informatics*, 81 (2012), pp. 579-93; C. Paul et al., 'Personal Health Records: Definitions, Benefits, and Strategies for Overcoming Barriers to Adoption', *Journal of the American Medical Informatics Association*, 3, pp. 121-26.

(2) Cfr. R. Dick, E. B. Steen, D. Demeter, 'The Computer Based Patient Record: An Essential Technology for Health Care', *Institute of Medicine, National Academy Press*, 1997, p. 111; A.B. Summerfield, S. Empey, 'Computer-based information systems for medicine: a survey and brief discussion of current projects.', 1965.

(3) Per tutti K. Häyrinen, K. Saranto, P. Nykänen, 'Definition, structure, content, use and impacts of electronic health records: a review of the research literature.', *International journal of medical informatics*, 77 (2008), pp. 291-304.

(4) International Standardization Organization, *Health informatics — Electronic health record — Definition, scope, and context*, 2005, ISO/TR 20514:2005(E).

in quattro differenti forme (5), "*Digital Medical Record*" (DMR) (6), "*Clinical Data Repository*" (CDR) (7), "*Computerised Medical Record*" (CMR) (8) e "*Population Health Record*" (PHR) (9). Tornando alla più generica definizione di Fascicolo Sanitario Elettronico (10), ci si deve necessariamente riferire alla definizione, stabilita a livello normativo dall'art. 12 del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221: "*il Fascicolo Sanitario Elettronico (FSE) è l'insieme dei dati e documenti digitali di tipo sanitario e sociosanitario generati da eventi clinici presenti e trascorsi, riguardanti l'assistito*". In particolare, ci si riferisce (senza particolari riferimenti architetturali) ad una raccolta di dati medici in formato elettronico (la storia clinica del paziente (11)) finalizzata a migliorare i livelli di servizio di cura e assistenza sanitaria (12). La

---

(5) "*a) a self-contained EHR, maintained and controlled by the patient/consumer, b) the same as a. but maintained by a third party such as a web service provider, c) a component of an ICEHR maintained by a health provider (e.g. a GP) and controlled at least partially (i.e. the PHR component as a minimum) by the patient/consumer, or d) the same as c) but maintained and controlled completely by the patient/consumer*".

(6) Si tratta di una cartella "*web-based*", gestita dal servizio sanitario, che può assolvere funzioni di EMR, EPR o EHR. Cfr. P. WAEGEMANN, 'Status Report 2002: Electronic Health Records' (Medical Records Institute, 2002).

(7) Composto di dati sanitari organizzati e provenienti dai servizi sanitari territoriali (ospedali o cliniche), che possono anche alimentare il Fascicolo Sanitario Elettronico.

(8) In esso, la documentazione raccolta nelle cartelle sanitarie cartacee è acquisita mediante i sistemi ottici di riconoscimento dei caratteri.

(9) Creato *ex novo* oppure direttamente dai fascicoli sanitari elettronici, nel quale, invece, dati aggregati, e comunque resi anonimi, sono utilizzati in sanità pubblica.

(10) Puntuali definizioni si trovano anche in D. GARETS, M. DAVIS, 'Electronic Patient Records. EMRs and EHRs', *Healthcare Informatics*, 4 (2005).

(11) La tipologia di informazioni sanitarie contenute nel FSE è piuttosto diversificata (al pari delle quanto avviene per le cartelle sanitarie cartacee). In tal senso: "*Operational EHRs include information such as observations, laboratory tests, diagnostic imaging reports, treatments, therapies, drugs prescribed, dispensed and administered, patient identifying information and demographics, legal permissions, allergies and the identities of healthcare professionals and provider organisations who have provided healthcare. This information is stored in various electronic formats using a multitude of medical information systems available on the market*", In M. EICHELBERG et al., 'Electronic Health Record Standards — a brief overview, conference paper for Information Processing in the Service of Mankind and Health', *ITI 4th International Conference on Information and Communications Technology*, 2006.

(12) A ciò si aggiunga che, in ossequio al principio di necessità (oggi confermato e assorbito dal principio "*data protection by design e by default*"), il FSE è costituito

peculiarità delle informazioni (dati relativi alla salute) contenute nel FSE impone requisiti di completezza, attendibilità, integrità, immodificabilità e, soprattutto, riservatezza, quindi adeguate misure di sicurezza (13) affinché non si configurino lesioni dei diritti fondamentali della persona.

2. *Le principali tappe dell'*iter *normativo (e operativo) in ambito FSE*

La realizzazione e diffusione sul territorio nazionale di una soluzione federata di Fascicolo Sanitario Elettronico del cittadino, in linea con lo scenario internazionale è uno dei principali interventi dell'Agenda digitale Italiana per l'attuazione della sanità digitale (14). Esso rappresenta uno strumento fondamentale per il miglioramento generale di tutte le attività assistenziali e di cura, attraverso l'offerta di un servizio che può facilitare l'integrazione delle diverse competenze professionali e, contestualmente, fornire una base informativa consistente.

La storia del lungo percorso normativo del FSE risale al secondo semestre del 2008, quando il Ministero della salute istituì un Tavolo interistituzionale con la finalità di uniformare su tutto il territorio nazionale i progetti regionali in essere dedicati al Fascicolo sanitario elettronico. A quel tavolo partecipavano esperti interni ed esterni del Ministero, rappresentanti del Dipartimento dell'innovazione della Presidenza del Consiglio dei Ministri (oggi AgID), referenti regionali ed un rappresentante dell'Autorità Garante per la protezione dai dati personali. Fu tale consesso ad elaborare una proposta normativa di disciplina uniforme per il FSE a livello nazionale. Dallo stesso gruppo furono

---

preferendo, di regola, soluzioni che non prevedono una duplicazione in una nuova banca dati delle informazioni sanitarie formate dai professionisti od organismi sanitari che hanno preso in cura l'interessato.

(13) Cfr. I. Iakovidis, 'Towards Personal Health Record: Current situation, obstacles and trends in im-plementation of Electronic Healthcare Records in Europe', *International Journal of Medical Informatics*, 128 (1998), pp. 105-17; M. G. Virone, *Il fascicolo sanitario elettronico. Sfide e bilanciamenti fra semantic web e diritto alla protezione dei dati personali* (Ariccia: Aracne, 2015).

(14) Tra gli altri interventi ritenuti fondamentali, vi è la digitalizzazione del ciclo prescrittivo, con l'introduzione della trasmissione delle certificazioni di malattia online e la sostituzione delle prescrizioni cartacee con l'equivalente documento digitale; l'aumento del grado di innovazione digitale nelle aziende sanitarie, sia nei processi di organizzazione [illegible] cittadini.

Capitolo III
IL VIAGGIO DELL'*E-HEALTH* VERSO LA "NUVOLA"

Sommario: 1. I principali vantaggi della migrazione in *cloud*. — 2. Le principali criticità. — 2.1. La circolazione dei dati sanitari: le regole generali. — 2.2. La legge applicabile. — 3. I più significativi contributi istituzionali dedicati al *cloud computing* (anche) in ambito sanitario. — 4. La Carta di Castelfranco. — 4.1. Le raccomandazioni della Carta di Castelfranco. — 4.2. Il *management* del *cloud*. — 4.3. Il rapporto del *cloud provider* con il mondo sanitario. — 5. Il rapporto dell'ENISA sul *cloud* in sanità: "*security and resilience in governmental clouds and in eHealth infrastructures & services*". — 5.1. Controllo e governo sui dati. — 6. L'indagine pilota sui servizi sanitari in Piemonte del centro NEXA su *internet* e società del politecnico di Torino. — 6.1. Contesto di riferimento e stato dell'arte. — 7. Questioni di *privacy* e *security* nel trattamento delocalizzato dei dati sanitari: la più recente disciplina europea in materia di trasferimento dei dati personali (anche sanitari) all'estero. — 7.1. Trasferimento di dati personali verso gli USA: dal *Safe Harbor* al *Privacy Shield*. — 8. Difficoltà di inquadramento soggettivo. — 9. Contromisure per la sicurezza dei dati personali: i parametri per la scelta del fornitore e la qualificazione AgID per il *cloud* nella P.A.. — 9.1. I meccanismi di certificazioni nel Regolamento. — 9.1.1. *Segue.* Gli standard ISO/IEC della "nuvola".

1. *I principali vantaggi della migrazione in* cloud

Al pari di ogni settore della P.A., anche per la sanità pubblica, organismo dotato di una struttura complessa ed articolata, sono numerosi i benefici che possono derivare dall'adozione delle tecnologie *cloud*.

Da una parte, si distinguono vantaggi di tipo organizzativo, che consistono nella sistematizzazione delle infrastrutture, nella riorganizzazione dei flussi informativi e conseguentemente, nel miglioramento della fruibilità dei dati all'interno del sistema. Dall'altra, quale diretta conseguenza dei primi, vi sono indubbi vantaggi economici e razionalizzazione dei costi, dovuti alla presenza di servizi più moderni, più efficienti e più funzionali.

Non è un caso che anche il DigitPA in passato si sia espresso in modo favorevole nei confronti del *cloud*, definendolo come uno dei mezzi più economici per assicurare ad una gran parte dei servizi di *e-government* caratteristiche di efficacia, efficienza, trasparenza, partecipazione, condivisione, cooperazione, interoperabilità e sicurezza.

Le infrastrutture *cloud* consentono di abbandonare le vecchie logiche legate all'uso di grandi e potenti macchinari, come accadeva con i *mainframe* o i *data center* locali, che necessitavano di competenze e risorse umane in grado di gestirli e quindi di rilevanti spese.

Per sua natura, la tecnologia di *cloud computing* è molto più semplice e facilmente integrabile con l'infrastruttura esistente: le applicazioni sono generalmente accessibili tramite un semplice *web browser* e ciò le rende quasi completamente indipendenti dai sistemi già in uso presso l'Ente; a ciò si aggiunga il vantaggio pratico della semplicità di configurazione, di avvio e di gestione. Inoltre con il *cloud*, a differenza di quanto accadeva in passato, l'Ente che intende aggiornare la propria infrastruttura IT non deve più verificare la compatibilità dei propri *server*, dei *client* e dei sistemi operativi utilizzati: attraverso l'utilizzo del *web browser*, che sostituisce il tradizionale rapporto *client-server*, le macchine già in uso all'Ente sono destinate ad una vita più lunga in quanto non è più necessaria una potenza sempre maggiore di elaborazione. Infatti, le infrastrutture condivise su cui vengono ospitate le applicazioni *cloud* sono progettate per garantire un'erogazione costante di potenza elaborativa all'aumentare delle istanze applicative e del numero di utenti attivi.

Il *cloud* implica il superamento totale del concetto di aggiornamento del *software* in uso e di tutto ciò che ne consegue in termini organizzativi, di sicurezza e di costi, in quanto le applicazioni in *cloud* vengono aggiornate direttamente dal fornitore del servizio sull'infrastruttura condivisa (nella quale risiedono), dopo accurati collaudi effettuati "*off-line*".

Inoltre, le infrastrutture di *cloud computing* assicurano la cosiddetta *Business Continuity* (o continuità operativa) (1), ossia prevedono

---

(1) L'Art. 50-*bis* del CAD, prevede che le amministrazioni predispongano dei piani di emergenza in grado di assicurare la continuità delle operazioni indispensabili per il servizio e il ritorno alla normale operatività. Il principio è quello della continuità operativa e obbliga le amministrazioni ad effettuare una valutazione preliminare sulle garanzie offerte dagli stessi *cloud provider*. Infatti, tra gli adempimenti della Pubblica Amministrazione, è prevista la definizione di un piano di continuità operativa, sotto-

modalità di ripristino di emergenza più rapide ed efficaci, nonché tempi di inattività dovuti a malfunzionamenti e/o manutenzione straordinariamente bassi. Infine, la gestione dei dati in *cloud* consente alle amministrazioni sanitarie di mettere in condivisione le proprie informazioni con altre strutture pubbliche, rendendo più efficiente il sistema attraverso un accesso rapido alle stesse.

Tutto ciò conduce verso un notevole risparmio economico, per lo meno sui costi di gestione ed amministrazione dell'infrastruttura IT.

Questo perché, in primo luogo, le spese di mantenimento e di aggiornamento dei *software* restano a carico del *cloud provider*; in secondo luogo perché la flessibilità dei servizi offerti in soluzioni *cloud*, consente all'Amministrazione di investire solo in caso di necessità e, quindi, le restanti risorse economiche possono essere utilizzate per altri investimenti ritenuti più urgenti.

Il risparmio nei costi di acquisto dell'*hardware* e del *software* è riscontrabile anche nel valore economico dei canoni d'uso, che risultano essere notevolmente inferiori al costo (2) totale delle licenze d'uso delle applicazioni *client-server* analoghe. Le applicazioni in *cloud*, infatti, non necessitano di un'infrastruttura centrale dedicata, i cui costi per l'alimentazione elettrica di funzionamento e di condizionamento superano di gran lunga quelli di acquisto. Inoltre, i grandi *cloud provider*, a differenza degli operatori locali, possono collocare le proprie sedi in luoghi dove il costo dell'energia è più favorevole, così da poter ridurre ulteriormente il canone del servizio.

Infine, vi è un ulteriore aspetto vantaggioso (meno immediato di quelli appena illustrati) costituito dalla riduzione della spesa per il lavoro umano da dedicare alla gestione dell'infrastruttura. Con il *cloud computing* non è necessario, ad esempio, un amministratore di sistema per ogni singolo *server*, bensì sarà sufficiente un unico professionista che segue contemporaneamente più *cloud server*, anche di clienti diversi e/o eterogenei (pubblici e privati).

---

posto a verifica biennale, che fissa gli obiettivi e i principi da perseguire, descrive le procedure per la gestione della continuità operativa, anche affidate a soggetti esterni. Il piano tiene conto delle potenziali criticità relative a risorse umane, strutturali, tecnologiche e contiene idonee misure preventive. Pertanto, nel caso in cui i servizi offerti in *cloud* non assicurino la sicurezza dei dati, affinché sia comunque rispettato l'obbligo previsto dall'Art. 50-*bis* del CAD, sarebbe opportuno che le Pubbliche Amministrazioni conservino *in house* una copia di tutti i dati immessi nella rete *cloud*.

(2) Tale costo va calcolato sommando il prezzo delle singole licenze d'uso, degli aggiornamenti periodici, dei contratti di manutenzione *software*.

2. *Le principali criticità*

Prima di affrontare nel merito gli aspetti critici della materia, risulta utile, per addivenire a una più completa comprensione, ripartire dalla definizione di *cloud computing* (3).

La computazione "nuvolare" rappresenta un concetto molto ampio, utilizzato spesso per definire genericamente la virtualizzazione o l'esternalizzazione dei servizi e delle attività. In assenza di una definizione normativa del *cloud*, è necessario rifarsi a due autorevoli definizioni di *cloud computing*, certamente utili in questa sede. La prima è la definizione ufficiale del *National Institute of Standards and Technology* (*NIST*) afferma che "*cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction*" (4);

La seconda definizione è quella elaborata dall'Autorità Garante per la protezione dei dati personali per la quale con l'espressione *cloud computing* si fa riferimento a un insieme di tecnologie e di modelli di servizio che "*favoriscono la fruizione e l'erogazione di applicazioni informatiche, di capacità elaborativa e di stoccaggio via* web*; promuovono a seconda dei casi il trasferimento dell'elaborazione o della sola conservazione dei dati dai computer degli utenti ai sistemi del fornitore dei servizi*" (5).

Alla luce delle definizioni riportate e delle caratteristiche tecniche

---

(3) F. Bassanini, E. Belloni, *L'impatto del cloud computing sull'economia Italiana* (Roma: Astrid, 2011), pp. 12 ss.; gli Autori sottolineano che non si tratta di una nuova tecnologia, ma di un « nuovo modo di organizzare e rendere fruibili tecnologie esistenti, integrandone le componenti e presentando all'utente solo le funzioni d'uso ». Sulla disamina del *cloud computing* come *quid pluris* rispetto a una mera sintesi verbale si rimanda a G. Reese, *Cloud Computing. Architettura, infrastrutture, applicazioni* (Milano: O'Reilly, 2010).

(4) "*Il* cloud computing *è un ambiente di esecuzione elastico che consente l'accesso via rete e su richiesta ad un insieme condiviso di risorse di calcolo configurabili (ad esempio rete, server, dispositivi di memorizzazione, applicazioni e servizi) sotto forma di servizi a vari livelli di granularità. Tali servizi possono essere rapidamente richiesti, forniti e rilasciati con minimo sforzo gestionale da parte dell'utente e minima interazione con il fornitore*", in P. Mell, T. Grance, 'The NIST Definition of Cloud Computing: Recommendation of the National Institute of Standards and Technology', 2011.

(5) Garante per la protezione dei dati personali, 'Cloud computing, proteggere i dati per non cadere dalle nuvole'.

Capitolo IV
I CONTRATTI DEL CLOUD COMPUTING

Sommario: 1. Il rapporto tra il contratto di *cloud computing* e la "categoria" dei contratti informatici. — 1.1. I confini comuni. — 1.2. Breve indagine sulla natura giuridica del contratto di *cloud*. — 1.3. Tentativi di inquadramento. — 1.3.1. Tra l'appalto di servizi e la licenza d'uso. — 1.3.2. I contratti *Software as a Service*. — 1.3.3. La "locazione" di spazio *web*. — 1.3.4. *Cloud* e *outsourcing* a confronto. — 1.3.5. La centralità dei dati come elemento di classificazione negoziale: il contratto di deposito di beni digitali. — 2. Profili contenutistici. — 3. Titolarità del dato e responsabilità connesse. — 4. Le clausole limitative della responsabilità del fornitore.

1. *Il rapporto tra il contratto di* cloud computing *e la "categoria" dei contratti informatici*

L'assenza di una disciplina positiva specificatamente dedicata ai contratti di *cloud computing* impone, come di regola accade ogni volta che si approccia la materia dei contratti legati alle tecnologie informatiche e telematiche, il ricorso — laddove possibile — alle norme già vigenti nell'ordinamento italiano *riferibili alla categoria dei contratti informatici*, anche se non dettate con specifica attenzione per questa tecnologia (o meglio, tenuto conto delle molteplici varianti del *cloud computing*, per queste fattispecie).

Alla base del *cloud computing*, come si è avuto modo di illustrare nelle prime due parti del presente lavoro, non c'è nulla di completamente nuovo, in quanto la sua logica è la medesima dei servizi *on-line*, tradizionalmente erogati ai consumatori finali (tramite *e-mail* e *social networks*), ma con la peculiarità di rivolgersi al mondo del *business* e della Pubblica Amministrazione attraverso la sostituzione di *hardware* e *software* con collegamenti *on-line* verso centri (banche dati) remoti. In sintesi, il *cloud computing* è un nuovo modo di fornire risorse, non una nuova tecnologia.

Ci si trova, pertanto, dinnanzi ad un contesto che, considerato nei singoli frammenti che lo compongo, non è nuovo per il mondo dei

giuristi che si sono occupati diffusamente di contratti informatici (1). Per questa ragione, l'analisi compiuta in questa sezione non può prescindere da un breve *excursus* sul contratto informatico, le cui caratteristiche si ripresentano anche per i qui esaminati.

1.1. *I confini comuni*

Il primo aspetto da considerare è proprio collegato alla difficoltà di definire un'unica categoria di contratti informatici. Si tratta, infatti, più precisamente, di molteplici fattispecie negoziali connesse a beni e

(1) Tra le autorevoli voci che si sono occupate dei contratti informatici, si vedano, per tutti: M. Iaselli, *I contratti informatici (III edizione)* (Altalex, 2015); G. Alpa, 'I contratti di utilizzazione del computer', *Giurisprudenza italiana*, 1983, pp. 42 ss.; G. Arnò, 'I contratti relativi all'hardware', *I contratti*, 1995, pp. 224 ss.; A. Braggion, 'La validità delle clausole che limitano od escludono la responsabilità nei contratti per la fornitura di software: una rassegna di recenti pronunzie nella giurisprudenza europea', *Rivista di diritto industriale*, 1 (1989); F. Bravo, 'Appalti pubblici per la fornitura di beni e servizi nel settore ICT e tecniche di redazione contrattuale. Le linee guida del CNIPA', *Diritto dell'informazione e dell'informatica*, 23 (2007), pp. 103 ss.; P. Cerina, 'Contratti internazionali di informatica e Legge applicabile, prime considerazioni', *Diritto dell'Informazione e dell'Informatica*, 1994, pp. 405 ss.; R. D'Arrigo, 'Prospettive della c.d. licenza a strappo nel nostro ordinamento', *Il diritto dell'Informazione e dell'Informatica*, 1996, pp. 462-68; G. Falletti, 'Il contratto di application service providing', *Il Diritto dell'Informazione e dell'Informatica*, 2001, pp. 411 ss.; M. Maggi, 'Il contratto di fornitura di sistema informatico come contratto indeterminato, nota a Cass. Sez. II, 22 marzo 1999, n. 2661', *I Contratti*, 1999, pp. 995 ss.; A. Musella, 'Il contratto di *outsourcing* del sistema informativo', *Diritto dell'informazione e dell'informatica*, 1998, pp. 857 ss.; C. Piana, 'Licenze pubbliche di software e contratto', *I Contratti*, 7 (2006), pp. 720-27.; M. Ricolfi, 'I contratti dell'informatica', reperito all'URL: www.jus.unitn.it/cardozo/review/Contract/Ricolfi-1998/sena1.htm; C. Rossello, 'La responsabilità da inadeguato funzionamento di programmi per elaboratori elettronici. Aspetti e problemi dell'esperienza nord americana', *Rivista critica del diritto privato*, 1984; R. Roversi, 'I contratti di *outsourcing* della manutenzione', *Contratto e Impresa*, 1997, pp. 522 ss.; P. Sammarco, 'Appalto di software e trasferimento di diritti', *Giustizia civile*, 1998, pp. 97 ss.; F. Sammartano, *I contratti informatici*, reperito all'URL: www.diritto.it/articoli/civile/ sammartano.html; M. Scuffi, 'I Contratti per la manutenzione: verso il "global service', *Diritto Industriale*, 1996, pp. 344 ss.; E. Tosi, 'Brevi note a margine del problema della qualificazione e dell'inadempimento del contratto di fornitura di hardware e software, nota a Tribunale di Bari, 4 giugno 1994', *Il Diritto dell'informazione e dell'informatica*, 11 (1995), pp. 933-37; E. Tosi, 'Natura e qualificazione dei contratti di fornitura dei sistemi informatici, nota a Tribunale Torino, 13 marzo 1993', *Il Diritto dell'Informazione e dell'Informatica*, 11 (1995), 386-98; A. Zaccaria, 'La responsabilità del produttore di software', *Contratto e impresa*, 1993, pp. 294 ss.

servizi rientranti nel comparto dell'informatica per le quali, al di là di questo debole comune denominatore, non è individuabile una *ratio* comune.

L'inquadramento giuridico dei contratti informatici ha risvolti notevoli anche relativamente ai contratti di *cloud*, per i quali "*diviene arduo individuare le giuste tecniche per garantire la sicurezza dell'elaborazione, conservazione, estrazione, condivisione, circolazione dell'informazione dotata di valore giuridico (come gli atti di un'amministrazione sanitaria). Diviene altrettanto arduo comprendere e normare la gestione dei flussi informativi, l'elaborazione e comunicazione della conoscenza internamente alle strutture sanitarie e tra queste e il cittadino/paziente*" (2).

Nonostante la dichiarata disomogeneità dei contratti informatici, spesso capita di imbattersi in fattispecie dai connotati comuni, tra i quali, il primo da ricordare, tipico anche dei negozi di *cloud*, è il notevole squilibrio di forza contrattuale che sussiste tra fornitore e cliente (3). Ne consegue che i contratti informatici non sono frutto di un accordo fra le parti, quanto piuttosto un mezzo attraverso il quale il soggetto più forte vincola il soggetto più debole (4), con la conseguenza che risulta indispensabile in ogni ordinamento apprestare strumenti che consentano un controllo sostanziale ed un maggior equilibrio degli interessi contrapposti.

Nella prassi commerciale i contratti di *cloud computing* sono predisposti unilateralmente dai *cloud providers*, i quali non sempre forniscono tutte le informazioni necessarie in merito alla collocazione dei *server* o alle misure di sicurezza adottate e non esplicitano chiaramente le garanzie offerte al fruitore dei servizi da loro erogati, riservandosi ampi poteri e prevedendo clausole di esclusione della propria responsabilità (5),. Sebbene la scarsa trasparenza e la carenza di garanzie tipica di questi contratti può non rappresentare un aspetto

---

(2) M. MANCARELLA, *cit.* p. 216.

(3) Sul ruolo delle parti si è già detto in precedenza, nella parte dedicata alla difficoltà di inquadramento soggettivo".

(4) Sulle problematiche connesse alla contrattazione standardizzata, in merito sua conformità ai alla teoria volontaristica secondo cui "la volontà è determinante degli effetti: qui sta la caratteristica propria del negozio giuridico", si veda per tutti E. ROPPO, *Contratti standard. Autonomia e controlli delle attività negoziali d'impresa.* (Milano: Giuffrè, 1975).

(5) La contrattazione in cui una delle parti ha soltanto il potere di aderire al programma negoziale predisposto unilateralmente dalla controparte comporta dei

rilevante per un utente che utilizza il *cloud* per scopi personali, dinnanzi ad un contratto che vede coinvolti enti pubblici, imprese o professionisti, che sono tenuti ad osservare precisi obblighi di legge, questi aspetti non possono essere tollerati. La Pubblica Amministrazione, ad esempio, deve sottostare alla disciplina dei contratti pubblici e potrebbe, a causa di un contenuto negoziale imposto dal *cloud provider*, non garantire la necessaria coerenza alle disposizioni (6).

Tutti i fruitori di servizi in *cloud* devono, quindi, essere consapevoli dei rischi e delle vulnerabilità della tecnologia che utilizzano anche e soprattutto sotto il profilo delle implicazioni giuridiche.

L'asimmetria tra le parti non deriva sempre dalla differente forza economica dei contraenti. La grande diffusione del *cloud computing*, infatti, coinvolge spesso, quali fruitori del servizio, soggetti tutt'altro che deboli, come ad esempio le Pubbliche Amministrazioni (anche di notevoli dimensioni). In materia di contratti informatici, poi, tra le parti si creano anche delle disparità di natura diversa da quelle sopraccitate: sono disarmonie legate alla cultura informatica delle parti e ciò incide inevitabilmente sulla consapevole predisposizione ovvero accettazione del programma negoziale.

Nell'ordinamento italiano, un correttivo a tale problema è rappresentato dagli obblighi di corretta informazione, che sussistono sia nella fase precontrattuale, in base al disposto dell'art. 1337 c.c., sia nella fase di esecuzione del contratto in base al generale dovere di correttezza e di buona fede di cui all'art. 1375 c.c.: la violazione di tali obblighi determina, nel primo caso, una responsabilità precontrattuale che può determinare anche l'annullabilità del contratto, qualora sia configura-

---

rischi ben noti da tempo. Per tutti, si veda G. Alpa, *Tutela del consumatore e controlli sull'impresa* (Bologna: Il Mulino, 1977).

(6) AgID, *Raccomandazioni e proposte sull'utilizzo del cloud computing nella Pubblica Amministrazione*, cit. p. 19. Con specifico riferimento alla materia dei contratti pubblici, va specificato che le Raccomandazioni sopraccitate sono state pubblicate sotto la vigenza del D.Lgs. 12 aprile 2006, n. 163 e del Regolamento attuativo D.P.R. n. 207/2010, che di recente sono stati espressamente abrogati dall'articolo 217, comma 1, del Decreto Legislativo 18 aprile 2016, n. 50 "*Attuazione delle direttive 2014/23/UE, 2014/24/UE e 2014/25/UE sull'aggiudicazione dei contratti di concessione, sugli appalti pubblici e sulle procedure d'appalto degli enti erogatori nei settori dell'acqua, dell'energia, dei trasporti e dei servizi postali, nonché per il riordino della disciplina vigente in materia di contratti pubblici relativi a lavori, servizi e fornitu*re". Pertanto, auspicando il pronto rilascio di una nuova versione (quella attualmente pubblicata è la 2.0), la lettura odierna delle Raccomandazioni di AgID va aggiunta temperata dal conto delle intervenute modifiche normative, con le [illegible] per le sole parti compatibili.

Capitolo V
OPEN DATA E RIUSO DEI DATI SANITARI

Sommario: 1. I dati al centro dei sistemi informativi sanitari. — 2. "*Privacy Enhancing Technology*" e *E-Health*. — 3. Il processo di apertura dei dati e interoperabilità. — 4. Gli "*Open Data*" e i "*Big Data*" in ambito sanitario.

1. *I dati al centro dei sistemi informativi sanitari*

Nell'ambito dei sistemi informativi sanitari il dato sanitario ricopre un ruolo centrale e di assoluta essenzialità per la tutela e la promozione della salute individuale e collettiva. Di fatto, l'informazione sanitaria rappresenta la base di partenza di ogni processo conoscitivo e, allo stesso tempo, contribuisce alla realizzazione di nuove informazioni e conoscenze. Questa evoluzione ciclica e, parallelamente, continua, consente all'informazione relativa allo stato di salute di svolgere un ruolo centrale all'interno dei processi diagnostico-terapeutici, sia per il singolo utente che per il sistema salute nel suo complesso. È possibile, infatti, riconoscere al dato sanitario una duplice funzione: quella di ausilio e cooperazione al miglioramento del "benessere fisico, psichico e sociale" (1) del paziente, da una parte, e quella di strumento per migiorare l'efficienza/efficacia del sistema sanitario, dall'altra.

È indubbio che il potenziale informativo riconosciuto ai dati sanitari debba essere massimizzato a vantaggio di tutti e della collettività, senza però trascurare il rispetto delle regole esistenti, sia tecniche che giuridiche; per realizzare ciò, è essenziale realizzare dei veri e

(1) Cfr. World Health Organization, 'Preamble to the Constitution of the World Health Organization as adopted by the International Health Conference n. 2', *Official Records of the World Health Organization*, 1946. A tal proposito, la salute è definita come "*a state of complete physical, mental and social well-being and not merely the absence of disease or infirmity*"; è importante sottolineare come la definizione, introdotta nel 1948 dal "*the International Health Conference*", ad oggi, non abbia subito alcuna modifica.

propri "modelli di armonizzazione" di norme, principi e metodologie adottabili non soltanto a livello locale, ma, soprattutto, a livello centrale ed europeo.

L'utilizzo del dato sanitario, come vettore per il miglioramento della salute personale e collettiva, assume connotazioni differenti in ragione della eterogeneità delle esigenze e delle richieste del paziente rispetto a quelle del sistema sanitario: per quanto concerne la posizione dell'assistito, le informazioni idonee a rivelarne lo stato di salute permettono al personale sanitario di attuare ogni azione necessaria alla cura della persona, mentre, per quanto riguarda, invece, il sistema sanitario, i dati sono acquisiti in forma aggregata e anonima (2) e, successivamente, elaborati da esperti e da *policy makers* al fine di predisporre azioni e politiche nell'interesse della collettività.

Il raggiungimento di entrambe le finalità attraverso l'utilizzo dei dati sanitari richiede dunque un approccio equilibrato, fondato su regole e norme in grado di garantire, da una parte, la tutela del consumatore (il paziente nell'ambito dei servizi sanitari) attraverso la protezione dei propri dati personali e, dall'altra, l'accessibilità, la sicurezza e l'usabilità dei dati sanitari per il perseguimento del fine collettivo. Sebbene tale approccio sia fondamentale tanto nell'uso del dato in ambito analogico che in quello digitale, con riferimento a quest'ultimo, tuttavia, è indispensabile dar vita a sistemi informativi che rispondano congiuntamente ai requisiti di *sicurezza* e *riuso*. Non vi è dubbio, infatti, che l'utilizzo di sistemi informativi digitali comporta maggiori rischi per i dati personali (con ulteriore aggravio per quelli di tipo sanitario), rispetto a quanto accade nei contesti basati sulla gestione analogica (cosiddetta cartacea). Di fronte a questa criticità, è doveroso sottolineare il diritto del paziente alla protezione delle informazioni personali (sanitarie), che lo riguardano, che si traduce nell'obbligo, per ciascun titolare di siffatti trattamenti, alla progettazione di infrastrutture informatiche idonee al perseguimento delle finalità prefissate e che siano, al contempo, dotate di misure di sicurezza in grado di tutelare il diritto fondamentale del paziente alla tutela della propria sfera personale.

Il trattamento del dato sanitario, oltre che finalità primarie di cura e assistenza del cittadino, può avere ulteriore utilità, se oggetto di riuso

---

(2) Per approfondire il concetto di anonimato, cfr. G. FINOCCHIARO, 'Anonimato (voce)', *Digesto delle Discipline Privatistiche-Sezione Civile aggiornamento*, 2010, pp. 12-20.

per il raggiungimento di finalità secondarie (come ad esempio, la ricerca clinica, epidemiologica, farmaceutica ecc.) e permettere, così, di allargare il campo di indagine, sia sotto il profilo qualitativo sia su quello quantitativo (3). In questo senso, è di assoluta utilità la possibilità di realizzare dati sanitari "aperti" (4) attraverso le informazioni già

(3) In materia di riutilizzo dell'informazione nel settore pubblico vedasi: *Direttiva 2003/98/CE del Parlamento europeo e del Consiglio del 17 novembre 2003* nonché Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni, *Riutilizzo dell'informazione del settore pubblico — Riesame della direttiva 2003/98/CE* -, Bruxelles, 7.5.2009, COM(2009) 212 definitivo.

(4) La definizione di "dati di tipo aperto" è contenuta nell'art. 1, comma 1, lett. l-*ter*) del D.Lgs. 82/2005. Si vedano anche le Linee guida per la stesura di convenzioni per la fruibilità di dati delle PA — art. 58 comma 2 del CAD (in https://www.agid.gov.it/sites/default/files/repository_files/linee_guida/linee_guida_convenzioni_fruibilita_dati_delle_pa_art_58_cad_0.pdf) e il Provvedimento del Garante Privacy n. 393 del 2 luglio (pubblicato sulla Gazzetta Ufficiale n. 179 del 4 agosto 2015), con il quale si individuano specifiche modalità e misure di sicurezza per lo scambio di dati tra Pubbliche Amministrazioni (con gli opportuni adattamenti al mutato assetto normativo ad opera, dapprima, del Reg. UE 2016/679 e, successivamente, del D.Lgs. n. 101/2018). L'art. 58 del CAD, nella sua precedente formulazione, prevedeva che l'accessibilità telematica ai dati delle pubbliche amministrazioni fosse regolata da "apposite convenzioni aperte all'adesione di tutte le Amministrazioni interessate volte a disciplinare le modalità di accesso ai dati da parte delle stesse Amministrazioni procedenti" (art. 58, comma 2, CAD). In seguito alle modifiche introdotte dal D.L. 24 giugno 2014, n. 90 (convertito, con modificazioni, dalla L. 11 agosto 2014, n. 114) ed alla successiva abrogazione dell'art. 58 del CAD, disposta dall'art. 64, comma 1, lettera k) del D.Lgs. 26 agosto 2016, n. 179, è cessato l'obbligo di predisporre le summenzionate convenzioni. Nonostante ciò, la stessa Autorità Garante, nel citato Provvedimento, ha ritenuto necessario prescrivere alle Pubbliche Amministrazioni, titolari di banche dati accessibili per via telematica, l'adozione delle convenzioni. Muovendo da tali considerazioni, è opportuno a regolare i rapporti di accesso alle raccolte informatiche di dati personali delle Pubbliche Amministrazioni mediante la stipulazione di apposite convenzioni, che tengano conto delle specifiche peculiarità di ciascun rapporto, e quindi delle finalità per le quali i dati personali vengono messi a disposizione, in modo da stabilire chiare condizioni e le modalità di accesso ai dati e garantire la protezione dei dati personali. A quanto detto, si aggiunga che nell'ambito del Regolamento, pur non essendo prevista alcuna forma di regolamentazione dei rapporti fra titolari autonomi, è richiesta l'adozione di specifiche misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, tenuto conto della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche (si veda l'art. 32 del RGPD). La convenzione, pertanto, si pone quale misura consigliata per garantire una più efficace tutela dei dati personali presenti nelle banche dati e per ridurre al minimo i rischi di accessi non autorizzati o di

a disposizione del Servizio Sanitario Nazionale nel suo complesso e unitamente a quelle raccolte nei Fascicoli Sanitari Elettronici dei cittadini. L'estensione delle finalità del trattamento dei dati contenuti nei FSE a motivi di studio e ricerca e motivi di salute pubblica, come si è già avuto modo di illustrare in precedenza, è già stato oggetto di intervento da parte del legislatore italiano, che con i D.Lgs. 179/2012 e del D.Lgs. 69/2013, ha espressamente manifestato la propria presa di coscienza anche sull'utilità degli usi secondari delle informazioni sanitarie (in forma anonima). In tal senso, in armonia con il Regolamento UE 2016/679, tra le tecniche di de-identificazione delle informazioni contenute nelle banche dati sanitarie, come il FSE, è importante preferire quelle che garantiscono l'anonimato rispetto a quelle di pseudonimizzazione, che presentano il costante rischio di ricostruibilità dell'identità dell'interessato, e che tali tecniche siano adottate come impostazione predefinita ("*by default*"), in modo da assicurare una maggiore garanzia in caso di uso secondario dei dati sanitari (5). Vanno disciplinate, in maniera precisa e puntuale, le modalità di utilizzo e protezione dei dati nei sistemi informativi soprattutto nel passaggio tra un sistema e l'altro, anche attraverso l'interoperabilità delle politiche di sicurezza, così da consentire, all'interno delle reti ospedaliere nazionali ed europee, la condivisione non solo della sicurezza dei sistemi ma anche degli obiettivi e degli strumenti utilizzati a tal fine.

Nella medesima direzione si è espresso recentemente il Consiglio d'Europa (6), con la già citata Raccomandazione del 27 marzo 2019 (7),

---

trattamenti non consentiti o non conformi alle finalità della raccolta dei dati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento. Il contenuto della convenzione, nonché le misure di sicurezza tecniche e organizzative adeguate, dovranno essere individuate nel rispetto dei principi generali e degli obblighi previsti dal Regolamento e dalle altre disposizioni applicabili in materia di protezione dei dati personali.

(5) Cfr. A. Cavoukian, R. C. Alvarez, *Embedding Privacy into the Design of EHRs to Enable Multiple Functionalities — Win/Win* (Toronto: Information and Privacy Commissioner of Ontario, 2012), pp. 19 ss.; A. Cavoukian, K. El Emam, *A Positive-Sum Paradigm in Action in the Health Sector* (Toronto: Information and Privacy Commissioner, Ontario, 2010), pp. 6 ss.

(6) Il Consiglio Europa (da non confondere con il Consiglio UE) è una organizzazione sovranazionale, oggi comprendente 47 Paesi, basata sul Trattato del 1952 (che Contiene anche la Carta Europea dei Diritti dell'Uomo).

(7) Recommendation CM/Rec(2019)2 of the Committee of Ministers to member States on the protection of health-related data, consultabile al seguente indirizzo web https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680093b26.

BIBLIOGRAFIA

Abdelhak, M. (1996). *Health Information Management of a Strategic Resource.* Philadelphia: W. B. Saunders Company.

Abet, F. (2007). Il ruolo delle tecnologie per una sanità moderna: la telemedicina. *Informatica & Documentazione, 51.*

Abeti, R. (2004). I nuovi contratti: nella prassi civile e commerciale.

Acquati, E., Macellari, S. & Osnaghi, A. (2012). Pubblica amministrazione che si trasforma: cloud computing, federalismo, interoperabilità., 2012. *Astrid, Osservatorio sul cloud computing nella pubblica amministrazione.*

Aguilar, L. J. (2012). CLOUD COMPUTING - Notes for a spanish cloud computing strategy. *Spanish Institute of Strategic Studies' Magazine*.

Alanazi, H. O. (2010). Securing electronic medical records transmissions over unsecured communications: An overview for better medical governance. *Journal of Medicinal Plants Research, 4*(19).

Alpa, G. (1977). *Tutela del consumatore e controlli sull'impresa.* Bologna: Il Mulino.

Alpa, G. (1983). I contratti di utilizzazione del computer. *Giurisprudenza italiana, IV*.

Amram, D. & Comandé, G. (2018). Sul non facile coordinamento degli obblighi imposti dal Regolamento europeo sulla protezione dei dati personali UE/679/2016 e dalla Legge n. 24/2017. *Rivista Italiana di Medicina Legale (e del Diritto in campo sanitario), 1.*

Anderson, J. G. (2000). Security of the distributed electronic patient record: a case-based approach to identifying policy issues. *International Journal of Medical Informatics, 60.*

Andreson, R. J. (1996). Security in Clinicas Infromation Systems. *University of Cambridge*.

Armellin, G., Betti, D., Casati, F., Chiasera, A., Martinez, G., & Stevovic, J. (2010, 9). Privacy preserving event driven integration for interoperating social and health systems. *Secure Data Management: 7th Vldb Workshop (SDM'10).*

Arnò, G. (1995). I contratti relativi all'hardware. *I contratti.*

Arnold, U. (2000). New dimensions of outsourcing: a combination of transaction cost economics and the core competencies concept. *European Journal of Purchasing & Supply Management, 6*(1), 23 ss.

Article 29 Data protection working party. (2007). Parere 4/2007 sul concetto di dati personali, adottato il 20 giugno, 01248/07/IT, WP 136.

Article 29 Data protection working party. (2007). Working Document on

the processing of personal data relating to health in electronic health records (EHR), adopted on 15 February 2007, 00323/07/EN, WP 131.

Article 29 Data protection working party. (2011). Opinion 15/2011 on the definition of consent, adopted on 13 July, 201101197/11/EN, WP187.

Article 29 Data protection working party. (2011). Thirteenth Annual Report on the situation regarding the protection of individuals with regard to the processing of personal data and privacy in the European Union and in third countries covering the year 2009, adopted on 14 July 2010.

Article 29 Data protection working party. (2012). Opinion 08/2012 providing further input on the data protection reform discussions WP199, 01574/12/EN.

Atelli, M., Aterno, S. & Cacciari, A. (2008). *Codice dell'amministrazione digitale. Commentario.* Roma.

Atienza, A. A., Hesse, B. W., Baker, T. B., Abrams, D. B., Rimer, B. K., Croyle, R. T. & Volckmann, L. N. (2007). Critical Issues in eHealth Research. *American Journal of Preventive Medicine, 32.*

Badger, L., Grance, T., Patt-Corner, R. & Voas, J. (2012). Cloud computing Synopsis and Recommendations. Recommendations of the National Institute of Standards and Technology. *NIST - Special Pubblication, 800*, 80-146.

Baker, G. R. & Norton, P. (2002). Patient Safety and Healthcare Error in the Canadian Healthcare System. A Systematic Review and Analysis of Leading Practices on Canada with Reference to Key Initiatives Elsewhere. A Report to Health Canada. *Healt Canada.*

Barnes, D. & Sakandar, B. (2005). *Cisco LAN Switching Fundamentals.* Ciscopress.

Bartoli, C. & Medaglia, M. (2012). Il riutilizzo dei dati nel settore della sanità pubblica: il progetto e-triage "triage on the cloud". *CATTID, Università Sapienza di Roma.*

Bassanini, F. & Belloni, E. (2011). *L'impatto del cloud computing sull'economia Italiana.* Roma: Astrid. Bassi, E. (2011). PSI, protezione dei dati personali, anonimizzazione. *Informatica e diritto*(1-2).

Bates, D., Teich, J. M., Lee, J., Seger, D., Kuperman, G., Ma'luf, N., Boyle, D., Leape, L. (1999).The impact of computerized physician order entry on medication error prevention. *Journal of the American Medical Informatics Association, 6*(4), pp. 313-321.

Battelli, E. (2011). Il nuovo Diritto europeo dei contratti nell'ambito della Strategia "Europa2020". *Contratti, XI.* Bazargan, F., Yeun, C. Y. & Semerly, M. J. (2012). State-of-the-Art of Virtualization, its Security Threats and Deployment Models. *International Journal for Information Security Research (IKISR), 2.*

Belisario, E. (2009). *La nuova Pubblica Amministrazione digitale. Guida al Codice dell'Amministrazione Digitale dopo la Legge n. 69/2009.* Rimini: Maggioli.

Belisario, E. (2011). Cloud Computing. *Informatica Giuridica - collana diretta da Michele Iaselli, eBook*(17).

Benci, L. (2017, 3). La trasparenza dei dati e la documentazione sanitaria.

Sicurezza delle cure e responsabilità sanitaria. Commentario alla legge 24/2017, 47-53.

Bendandi, S. (2008). Software as a Service (Saas): aspetti giuridici e negoziali.

Bennet, C. & Timbrell, G. T. (2000). Application Service Providers: Will They Succeed? *Information Systems Frontiers (ISF), 2*(2).

Berners-Lee, T. (2009). Is your Linked Open Data 5 Star?

Bernstein, K., Bruun-Rasmussen, M., Vingtoft, S., Andersen, S. K. & Nøhr, C. (2005). Modelling and implementing electronic health records in Denmark. *International Journal of Medical Informatics, 74.*

Bianca, C. M. (1997). *Il Contratto.* Milano: Giuffrè.

Birnhack, M. D. (2008). The EU Data Protection Directive: An engine of a global regime. *Computer Law&Security Report, 24.*

Blobel, B. & Pharow, P. (2009). Analysys and Evaluation of EHR Architecture. *Method Inf. Med., 2*, 162-169.

Bolognini, L., Fulco, D. & Pelino, E. (2012). Dati sanitari e Cloud Computing per finalità di triage di pronto soccorso: profili e criticità in materia di protezione dei dati personali. *Istituto Italiano per la Privacy.*

Bonavita S., Pardolesi R., "*GDPR e diritto alla cancellazione in Danno e responsabilità*, n. 3/2018, Ipsoa.

Bonazzi, E. & Triberti, C. (1990). *I contratti nell'informatica.* Milano: Ipsoa.

Borking, J. & Raab, C. (2001). Laws, PETs and Other Technologies for Privacy Protection. *The Journal od Information, Law and Technology, 1*, 1-14.

Bos', J. J. (1996). Digital signatures and the electronic health records: providing legal and security guarantees. *International Journal of Bio-Medical Computing.*

Bradshaw, S., Millard, C. & Walden, I. (2010, 9 1). Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services. *International Journal of Law and Information Technology.*

Braggion, A. (1989). La validità delle clausole che limitano od escludono la responsabilità nei contratti per la fornitura di software: una rassegna di recenti pronunzie nella giurisprudenza europea. *Rivista di diritto industriale, 1.*

Bravo, F. (2007). Appalti pubblici per la fornitura di beni e servizi nel settore ICT e tecniche di redazione contrattuale. Le linee guida del CNIPA. *Diritto dell'informazione e dell'informatica, 23*(1).

Breda, R. (2017). La responsabilità civile delle strutture sanitarie e del medico tra conferme e novità. *Danno e responsabilità*, 283 ss.

Brenna E. (2011). La valutazione economica delle tecnologie in sanità con particolare riferimento all'area della telemedicina. *Sanità Pubblica* (7-8).

Brennan, P. F., Downs, S. & Casper, G. (2010). Project HealthDesign: rethinking the power and potential of personal health records. *Journal of biomedical informatics, 43*(5), S3-S5.

Brighi, R. & Virone, M. G. (2014). Una tutela "by design" del diritto alla salute. Prospettive di armonizzazione giuridica e tecnologica. *A Matter of Design: Making Society trough Science and Technology.*

Brocade. (2010). Brocade One Data Center-Cloud-Optimized Networks, http://www.brocade.com/

Brooks, T. T., Caicedo, C. & Park, J. S. (2012). Security Vulnerability Analysis in Virtualized Computing Environments. *International Journal of Intelligent Computing Research (IJICR), 3*(1-2).

Brown, N. & Reynolds, M. (2000). Strategy for production and maintenance of standards for interoperability within and between service departments and other healthcare domains. Short Strategic Study CEN. *TC, 251*, 0-47.

Buccoliero, L., Caccia, C. & Nasi, G. (2005). *e-he@lth. Percorsi di implementazione dei sistemi informativi in sanità.* Milano: McGraw-Hill.

Buscemi, A. & Caccaro, A. (2011). L'innovazione tecnologica RFID a garanzia della sicurezza del paziente. *Diritto Sanitario Moderno, 59*.

Busnelli, F. D. (1979). *Il diritto alla salute.* (U. Breccia, a cura di) Bologna: Il Mulino. Busnelli, F. D. & Breccia, U. (1978). *Tutela del diritto alla salute e diritto privato.* Milano.

Buyya, R., Ranjan, R. & Calheiros, R. N. (2010). InterCloud: Utility-Oriented Federation of Cloud Computing Environments for Scaling of Application Services. *Algorithms and Architectures for Parallel Processing - Lecture Notes in Computer Science, 6081*.

Caccia, C. (2008). *Management dei sistemi informativi in sanità.* Milano: Mcgraw-hill.

Cagnasso, O. & Cottino, G. (2000). Contratti commerciali. In *Trattato di Diritto Commerciale Diretto da G. Cottino.* Padova.

Cagnasso, O. & Cottino, G. (2000). *Trattato di Diritto Commerciale.* Padova: CEDAM.

Cagnasso, O., Cottino, G., Bartolotti, A., Callegari, M. & Spiotta, M. (2000). *Contratti commerciali.* Padova: Cedam.

Callens, S. & Crolla, D. (2003). *E-health and the law.* Kluwer Law International. Calzolaio, S. (2017). *Protezione dei dati personali.* Dig. Giuffrè.

Cannon, D. S. & Allen, S. N. (2000). A comparison of the effects of computer and manual reminders on compliance with a mental health clinical practice guideline. *Journal of the American Medical Informatics Association, 7*(2).

Cardarelli, F. (1993). La cooperazione fra imprese nella gestione di risorse informatiche: aspetti giuridici del c.d. outsourcing. *Diritto dell'Informazione e dell'Informatica, I*, 85 ss.

Cardarelli, F. (1996). Efficienza e razionalizzazione dell'attivita amministrativa: i contratti ad oggetto informatico nella pubblica amministrazione. *Universita degli studi di Camerino, Centro int. le audiosivisi e stampa*.

Caringella, F. & Buffoni, L. (2015). *Manuale di diritto civile - V edizione.* Dike Giuridica Editrice.

Carlin, S. & Curran, K. (2011). Cloud Computing Security. *International Journal of Ambient Computing and Intelligence, 3*(1).

Carloni, E. (a cura di). (2005). *Codice dell'amministrazione digitale.* Rimini: Maggioli Editore.

Carrol, M., Kotzè, P. & van der Merwe, A. (2012). Securing Virtual and Cloud Environments. In *CloudComputing and Services Science* (p. 73-90). New York: Springer.

Cartabia, M. [illegible] Giuffrè. *Iustitia*, 2, 153-182.