UNIVERSITÀ DEGLI STUDI DI TRENTO
Dipartimento di Scienze Giuridiche

PAOLO GUARDA

FASCICOLO SANITARIO ELETTRONICO
E
PROTEZIONE DEI DATI PERSONALI

2011

UNIVERSITÀ DEGLI STUDI DI TRENTO

Dipartimento di Scienze Giuridiche

QUADERNI DEL DIPARTIMENTO

94

2011

La pubblicazione è realizzata nell'ambito del progetto "TreC: la cartella clinica del cittadino", finanziato dall'Assessorato alle Politiche per la Salute e dall'Assessorato alla Programmazione, Ricerca e Innovazione della Provincia autonoma di Trento. Gli Enti partecipanti al progetto sono: FBK-Fondazione Bruno Kessler di Trento e Dipartimento di Scienze Giuridiche dell'Università degli Studi di Trento.

ISBN 978-88-8443-370-1
ISSN 1972-1137

Maggio 2011

PAOLO GUARDA

FASCICOLO SANITARIO ELETTRONICO
E
PROTEZIONE DEI DATI PERSONALI

Università degli Studi di Trento 2011

a mio padre,
cui debbo la virtù antica dell'onore

INDICE

Pag.

Pag.

CAPITOLO II
IL QUADRO NORMATIVO ITALIANO

Pag.

Pag.

ABBREVIAZIONI ED ACRONIMI

AMR	*Automated Medical Record*
ANSI	*American National Standard Institute*
ARRA	*American Recovery and Reinvestment Act 2009*
ASL	Azienda Sanitaria Locale
CAD	d.lgs. 7 marzo 2005, n. 82, Codice dell'Amministrazione Digitale
CIE	Carta d'Identità Elettronica
CMR	*Computerised Medical Record*
CMS	*Centers for Medicare & Medicaid Services*
CNS	Carta Nazionale dei Servizi
Codice Privacy	d.lgs. 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali
DICOM	*Digital Imaging and Communication in Medicine*
DMP	*Dossier Médical Personnel*
Documento CCE art. 29	Documento di lavoro sul trattamento dei dati personali relativi alla salute contenuti nelle cartelle cliniche elettroniche (CCE), adottato il 15 febbraio 2007 dal Gruppo art. 29
EHR	*Electronic Health Record*

EMR	*Electronic Medical Record*
EPR	*Electronic Patient Record*
epSOS	*Smart Open Services for European Patients*
FSE	Fascicolo Sanitario Elettronico
Garante Privacy	Garante per la protezione dei dati personali
HHS	*Department of Health and Human Services*
HIE	*Health Information Exchange*
HIPAA	*Health Information Portability Accountability Act 1996*
HITECH	*Health Information Technology for Economic and Clinical Health Act 2009*
HL7	*Health Level Seven*
ICT	*Information and Communication Technologies*
IHE	*Integrating the Healthcare Enterprise*
IT	*Information Technology*
LG FSE	Linee guida in tema di Fascicolo Sanitario Elettronico (Fse) e di *dossier* sanitario – 16 luglio 2009
LG Referti	Linee guida in tema di referti *on-line* – 19 novembre 2009
MMG	Medico di medicina generale
NHS CRS	*NHS Care Record Service*

ONC	*Office of the National Coordinator for Health Information Technology*
PHR	*Personal Health Record*
PLS	Pediatra di libera scelta
PROREC	*Promotion Strategy for European Electronic Healthcare Record*
SSN	Servizio Sanitario Nazionale
TIC	Tecnologie dell'Informazione e delle Comunicazioni
TSE	Tavolo di lavoro permanente per la Sanità Elettronica

PREMESSA

L'opera monografica di approfondimento giuridico che si offre al lettore è il frutto di un cammino, umano e professionale, che ha segnato gli ultimi otto anni. Il tema del rapporto tra privacy, protezione dei dati personali e sicurezza ha caratterizzato fin dal principio il mio percorso di ricerca: lo studio contenuto nella tesi dottorale già riguardava un'analisi delle misure di sicurezza nel contesto della protezione dei dati personali in prospettiva comparata. Proprio in quel periodo ho avuto modo di approfondire la materia partecipando a convegni e seminari sul tema, redigendo alcune pubblicazioni scientifiche, ma soprattutto giovandomi dell'esperienza maturata durante alcuni soggiorni di ricerca all'estero: mi riferisco, in particolare, all'attività svolta presso la *School of Law - University of California* a Berkeley (luglio-agosto 2005) e presso l'*Instituut voor Informatierecht - Universiteit van Amsterdam* (dicembre 2006-gennaio 2007).

L'occasione di declinare quanto appreso in tema di sicurezza informatica e protezione dei dati personali nel contesto del trattamento digitalizzato dei dati sanitari ed, in particolare, in tema di Fascicolo Sanitario Elettronico è derivata dall'attività svolta in qualità di assegnista di ricerca presso il Dipartimento di Scienze Giuridiche dell'Università degli Studi di Trento, con la direzione scientifica di Umberto Izzo, nel quadro del progetto «La Cartella Clinica del Cittadino – TreC», finanziato dalla Provincia autonoma di Trento e il cui coordinamento tecnico-scientifico è curato dalla Fondazione Bruno Kessler attraverso l'Unità di ricerca applicata *eHealth*. Ho potuto, così, far tesoro delle riflessioni maturate nell'arco di diversi mesi in seno alle riunioni tenutesi nell'ambito del medesimo progetto. Il frutto tangibile degli sforzi com-

piuti per dare attuazione al modello trentino si ritroverà nel testo laddove sono stati forniti al lettore spunti di riflessione su possibili soluzioni pratiche volte a costituire un sistema di Fascicolo Sanitario Elettronico conforme ai principi propri della disciplina in materia di protezione dei dati personali; le opinioni espresse nel presente lavoro, però, sebbene ispirate da questo proficuo dialogo con la prassi, rappresentano convizioni personali di chi scrive.

La partecipazione come relatore ad alcuni convegni e seminari, anche a carattere internazionale, mi ha, infine, dato la preziosa possibilità di condividere idee ed opinioni con esperti della materia ed operatori del settore: mi riferisco, in particolare, al *Doctoral Workshop on Law and Technology*, organizzato presso l'*European University Institute*, Firenze, il 5 giugno 2009; al Seminario «Il fascicolo sanitario elettronico: tutele giuridiche e prospettive applicative», tenutosi presso la Facoltà di Giurisprudenza dell'Università degli Studi di Trento il 7 luglio 2009; al Convegno Internazionale *Comparative Issues in the Governance of Research Biobanks: Property, Privacy, Intellectual Property, and Role of Technology*, celebratosi a Trento nei giorni 7-8 maggio 2010.

Un grazie sentito va a tutte le persone con le quali ho avuto la possibilità di confrontarmi e discutere durante questi anni: anche attraverso i loro consigli e suggerimenti quest'opera ha potuto prendere forma. Tra tutti tengo a nominare Roberto Caso, Umberto Izzo e Giovanni Pascuzzi.

Infine, merita una menzione particolare Rachele che rende possibile ogni giorno tutto quello che faccio: solo al suo entusiasmo ed alla sua enorme pazienza nei momenti di difficoltà devo il concretizzarsi dei miei sogni.

INTRODUZIONE

Il fenomeno della digitalizzazione ha da tempo investito anche i dati sanitari. Questa considerazione, che può apparire banale, nasconde la necessità di analizzare con estrema attenzione il processo in atto al fine di poterlo valutare in tutta la sua portata e di poterne individuare problemi e criticità.

Momento decisivo di tale digitalizzazione è l'implementazione di sistemi di gestione dei dati posti in essere dalle aziende sanitarie al fine di potenziare le loro capacità di cura e prevenzione. Questi sistemi sono infrastrutture informatiche che prendono il nome di «Fascicolo Sanitario Elettronico» (FSE). Il FSE rappresenta un nuovo importante strumento a disposizione di chi opera nel mondo sanitario ed ospedaliero. Esso si sostanzia in due momenti fondamentali: da un lato, quello dell'archiviazione di una massa di dati ed informazioni; dall'altro, quello della condivisione dei dati così archiviati tra tutti gli operatori del sistema legittimati al trattamento.

All'interno del contesto italiano si registrano diverse esperienze locali concernenti l'informatizzazione della gestione dei dati sanitari che hanno affrontato il problema agendo, però, in «ordine sparso» e senza il necessario coordinamento. Anche in ambito europeo progetti di questo tipo cominciano ad essere discussi e portati avanti nelle fasi applicative. Spinte all'attuazione di un sistema di FSE provengono, altresì, da documenti e raccomandazioni approvate in contesti sovranazionali (come il «Documento di lavoro sul trattamento dei dati personali relativi alla salute contenuti nelle cartelle cliniche elettroniche (CCE)», adottato il 15 febbraio 2007 dal Gruppo di lavoro articolo 29 per la protezione dei dati personali).

In considerazione del fatto che questo tipo di infrastrutture determina l'emersione di numerose criticità in relazione alla normativa in materia di protezione dei dati personali (come noto contenuta, per quanto riguarda l'ordinamento italiano, nel d.lgs. 30 giugno 2003, n. 196, «Codice in materia di protezione dei dati personali») e che manca una norma legislativa di riferimento per il FSE, il Garante per la protezione dei dati personali è intervenuto tracciando le linee guida della materia. Il 5 marzo 2009 veniva varato un provvedimento a carattere generale avente ad oggetto le «Linee guida in tema di fascicolo sanitario elettronico e di *dossier* sanitario» e ne veniva contestualmente avviata la consultazione pubblica al fine di ricevere osservazioni e commenti entro il 31 maggio 2009. Il processo consultivo culminava, poi, nell'emanazione di un Provvedimento a carattere generale concernente «Linee guida in tema di Fascicolo Sanitario Elettronico (Fse) e di *dossier* sanitario – 16 luglio 2009». Di lì a poco il Garante interveniva su di un aspetto connesso al FSE, riguardante, nello specifico, l'attività di refertazione *on-line*. Vedeva, così, la luce il Provvedimento a carattere generale del 25 giugno 2009, recante «Linee guida in tema di referti *on-line*», anch'esso posto in consultazione pubblica e scaturente poi nelle definitive «Linee guida in tema di referti *on-line* – 19 novembre 2009».

L'avvento di una regolamentazione giuridica di dettaglio volta ad interpretare l'esigenza di apprestare una tutela rinforzata ai dati sanitari oggetto di trattamento attraverso il FSE segna oggi un punto di svolta nel faticoso processo di sviluppo della sanità elettronica in Italia. Si tratta di un momento di cruciale importanza: da tale quadro giuridico-concettuale discende l'ambito di applicazione di adempimenti ed accorgimenti attraverso i quali i diritti del cittadino-paziente-interessato saranno tutelati. Si tratta di rendere conforme all'ordinamento giuridico vigente il trattamento dei dati sanitari operabile per via elettronica da un ventaglio di soggetti (titolari) accomunati dal compito di realizzare una

finalità di cura volta a beneficiare in modo diretto il paziente-interessato a quei dati.

L'inquadramento teorico di ciò che deve intendersi per FSE condiziona le prospettive di sviluppo della sanità elettronica italiana, poiché una definizione inevitabilmente presuppone l'adozione di un modello concettuale mediante il quale pensare poi il rapporto fra l'informazione, il soggetto a cui essa si riferisce e gli operatori sanitari che la trattano. Ciò suggerisce di procedere con particolare cautela nell'elaborazione di un modello teorico di FSE, onde evitare che la scelta di una definizione troppo restrittiva possa precluderne il successivo sviluppo.

Così ragionando, una considerazione che s'impone in via preliminare è questa: il rinnovato ruolo (inter-)attivo che il paziente, mercé la tecnologia, può esercitare all'interno del sistema informativo al centro della nostra analisi è un dato che non può essere trascurato nello svolgimento dell'approfondimento che ci accingiamo a compiere. Come avviene in tutti gli ambiti della vita dell'uomo dove l'introduzione delle tecnologie digitali garantisce l'affermarsi di nuove possibilità di estrinsecazione delle relazioni sociali, anche in quello sanitario è richiesto all'utente-paziente di acquisire una sorta di alfabetizzazione informatica, per svolgere un ruolo di primo attore delle scelte curative e dei processi di cura che lo riguardano. La scommessa cruciale dei sistemi informatizzati in ambito sanitario sta nel riuscire a dare espressione a questa esigenza, coordinando ed incorporando all'interno delle infrastrutture quei principi giuridici che già nel contesto non digitale hanno lo scopo di assicurare l'integrità e la libertà dei consociati.

Il lavoro monografico contenuto nelle pagine che seguono intende far proprio un approccio metodologico basato sull'interdisciplinarità e, senza perdere in profondità, persegue l'obiettivo di costruire i presupposti per dialogare, oltre che con i giuristi, anche con medici, informatici, amministratori pubblici e privati, nonché con tutte le figure

professionali che, in generale, sono coinvolte nello sviluppo dei nuovi sistemi di sanità elettronica.

La trattazione si articola come segue.

Il primo capitolo mira a tracciare il panorama delle tecnologie e delle *policy* di riferimento per il FSE. Anzitutto, esso affronta lo studio della sanità elettronica e della digitalizzazione dei dati sanitari, cercando di fornire le fondamenta concettuali e metodologiche per meglio comprendere l'oggetto del presente lavoro. Specifica attenzione è dedicata all'analisi delle problematiche più prettamente informatiche che i sistemi di FSE presentano. Un aspetto fondamentale è sicuramente quello che riguarda gli standard della sanità elettronica: il successo e la reale efficacia di questi sistemi si giocano sulla condivisione di standard aperti al fine di garantire l'interoperabilità e l'interconnessione delle piattaforme digitali. Il capitolo si chiude con la descrizione di alcune esperienze locali ed estere in materia di FSE.

Il secondo capitolo entra nel vivo delle problematiche giuridiche ed affronta, sulla falsariga delle indicazioni del Garante, le questioni che emergono quando si decide di rendere operativi questi nuovi servizi di gestione informatizzata dei dati sanitari. La trattazione affronta i punti salienti del dibattito e prospetta, laddove possibile, alcune soluzioni applicative. L'ordinamento giuridico di riferimento è, evidentemente, quello italiano, ma le problematiche appaiono comuni a tutti i principali progetti di sanità elettronica di cui è dato scrutinare lo sviluppo nel contesto europeo.

Il terzo capitolo approfondisce alcuni aspetti notevoli e i principali nodi problematici che scaturiscono dall'incrocio tra FSE e protezione dei dati personali. Il fenomeno della gestione dei dati sanitari tramite questo nuovo tipo di piattaforma mette a nudo le criticità sottese ad alcuni concetti chiave della disciplina della privacy in ambito sanitario, offrendo il destro per ripensarne la formulazione. Il tentativo di dare corretta attuazione ai modelli di FSE, in conformità ai principi ed alle

regole propri della normativa in materia di protezione dei dati personali, evidenzia difficoltà interpretative che sono comuni a molti ambiti del diritto dell'era digitale. L'obiettivo è quello di sciogliere i dubbi più rilevanti.

La parte conclusiva dell'opera si concentra sul problema relativo all'individuazione dei criteri volti a determinare, all'interno di questi nuovi sistemi di gestione informatizzata dei dati sanitari, il corretto punto di contatto tra la necessità di garantire un ruolo da protagonista al paziente ed il riconoscimento di poteri di controllo e di accesso distribuiti tra le varie strutture sanitarie ed i diversi soggetti che hanno come dovere-obbligo la cura dei singoli e, più in generale, la salute di tutti.

CAPITOLO I

TECNOLOGIE E *POLICY*

1. Le tecnologie digitali in ambito medico

1.1 Cenni introduttivi

Prima dell'era digitale il trattamento dei dati sanitari si basava su un rapporto strettamente fiduciario tra paziente (*rectius*, interessato al trattamento) e medico, che nella più parte dei casi era il c.d. «medico di famiglia». Il tutto poi avveniva generalmente in modalità cartacea, quando non orale.

L'avvento dell'informatizzazione ha determinato l'emersione di nuove problematiche e di inedite esigenze di protezione. A fronte degli straordinari vantaggi legati alla possibilità di gestire rapidamente enormi quantità di informazioni aggregate, la digitalizzazione ha reso possibile la creazione di estese banche dati a cui sempre più soggetti – seppur limitati e specificatamente individuati – possono avere accesso. Ciò ha aumentato in maniera esponenziale i rischi legati al trattamento dei suddetti dati, alla loro illecita diffusione, alla possibilità di ledere la dignità e le libertà fondamentali della persona interessata al trattamento[1].

[1] In prima approssimazione sul tema della telemedicina, v. L. SARTORI, *La tutela della salute pubblica nell'Unione europea*, Cittadella, 2009, 116-121; U. IZZO, *Medicina e diritto nell'era digitale: i problemi giuridici della cibermedicina*, in *Danno e resp*., 2000, 807; A. SINHA, *An Overview of Telemedicine: The Virtual Gaze of Health Care in the Next Century,* in *Medical Anthropology Quarterly*, New Series, vol. 14, n. 3 (Sep., 2000), 291-309, in Rete: <http://www.jstor.org/stable/649500>. Per un'analitica descrizione dei vari strumenti ed applicazioni che le tecnologie digitali offrono in ambito me-

Per questi motivi il legislatore europeo – con le note direttive 95/46/Ce (tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati) e 2002/58/Ce (relativa al trattamento dei dati personali ed alla tutela della vita privata nel settore delle comunicazioni elettroniche)[2] – e quello nazionale – nel contesto italiano da ultimo con il già citato d.lgs. 30 giugno 2003, n. 196, «Codice in materia di protezione dei dati personali» (d'ora in avanti: Codice Privacy) – sono intervenuti, dedicando al problema del trattamento dei dati sanitari una disciplina *ad hoc*, con ciò evidenziando la specificità e la pericolosità che le operazioni aventi ad oggetto questa particolare categoria di dati possono determinare[3].

La sanità elettronica rappresenta un'importante innovazione in grado di migliorare l'accesso all'assistenza sanitaria e di rafforzare la

---

dico v. E. SANTORO, *web 2.0 e Medicina, Come social network, podcast, wiki e blog trasformano la comunicazione, l'assistenza e la formazione in sanità*, Roma, 2009.

[2] Così come modificata dalla recente Direttiva 2009/136/Ce del Parlamento europeo e del Consiglio del 25 dicembre 2009, recante modifica della Direttiva 2002/22/Ce relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica, della Direttiva 2002/58/Ce relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e del Regolamento (Ce) n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori.

[3] Per quanto riguarda la disciplina della protezione dei dati personali nel contesto europeo, si v., in prima battuta, I.J. LLOYD, *Information technology law*, V ed., Oxford, 2008, 1 ss.; N. LUGARESI, *Protezione della privacy e protezione dei dati personali: i limiti dell'approccio comunitario*, in *Giust. amm*., 2004, 289; R. PARDOLESI, *Dalla riservatezza alla protezione dei dati personali: una storia di evoluzione e discontinuità*, in R. PARDOLESI (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Milano, 2003, 1-57; L.A. BYGRAVE, *Data Protection Law. Approaching Its Rationale, Logic and Limits*, The Hague – London - New York, 2002; P. PALLARO, *Libertà della persona e trattamento dei dati personali nell'Unione europea*, Milano, 2002; P. GUARDA, *Data Protection, Information Privacy, and Security Measures: an Essay on the European and the Italian Legal Frameworks*, in *Ciberspazio e dir*., 2008, 65 (in Rete: <http://eprints.biblio.unitn.it/archive/00001524/>); M. MARTINES, *La protezione degli individui rispetto al trattamento automatizzato dei dati nel diritto dell'Unione europea*, in *Riv. it. dir. pubbl. com*., 2000, 719; J. MORTON, *Data Protection and Privacy*, 18 *European Intellectual Property Review* 558 (1996).

qualità e l'efficacia dei servizi offerti. Essa, infatti, consente sin d'ora di ottenere consistenti incrementi di produttività ed efficacia delle prestazioni offerte dal sistema sanitario, agevolando l'affermazione di sistemi sanitari avanzati sempre più attenti ai fabbisogni di salute del cittadino.

Da alcuni lustri la Comunità europea si preoccupa di promuovere programmi di ricerca sul tema. Numerosi risultati di questi sforzi sono già stati testati e messi in pratica. L'Europa si colloca, di conseguenza, in una posizione di tutto rilievo nell'utilizzo delle tecnologie digitali sia per finalità di assistenza sanitaria di base che per l'impiego del nuovo FSE.

Tutto ciò riflette una tendenza globale, in quanto i sistemi sanitari si trovano a far fronte a nuove impegnative sfide di portata sovranazionale[4].

Si assiste, anzitutto, ad una crescente domanda di servizi sociali e sanitari determinata da un progressivo invecchiamento della popolazione mondiale – specialmente nei Paesi occidentali – e da livelli di reddito e di istruzione più elevati rispetto al passato, che modificano l'approccio, anche cognitivo, dei cittadini-utenti al servizio sanitario.

Si deve poi registrare una sensibile evoluzione della domanda stessa di assistenza sanitaria. Il progresso tecnologico ha esteso il grado di efficacia e di sofisticazione dell'intervento medico determinando, così, un innalzamento delle aspettative sociali e, di conseguenza, più elevate pretese da parte dei pazienti, i quali sono anche portatori di nuove esigenze: un bisogno di salute avvertito in maniera sempre più evidente, un'aspettativa crescente nei confronti del sistema ed un maggior grado di informazione (c.d. alfabetizzazione informatico-sanitaria).

[4] Cfr. SARTORI, *La tutela della salute pubblica nell'Unione europea*, cit., 33-49; L. BUCCOLIERO, C. CACCIA, G. NASI, *e-he@lth. Percorsi di implementazione dei sistemi informativi in sanità*, Milano, 2005, 1-3.

Un altro fattore importante è sicuramente rappresentato dall'evoluzione del sistema di offerta, il quale risente da un lato della crescente difficoltà che connota l'azione della pubblica autorità nell'armonizzare gli investimenti in campo tecnologico con quelli destinati alla realizzazione di complesse riforme organizzative, dall'altro dalla necessità di riuscire a fornire la migliore assistenza sanitaria possibile disponendo di una dotazione finanziaria limitata.

Infine, la crescente mobilità di pazienti ed operatori, la quale, dando vita ad una sorta di *hospital shopping*, spinge gli utenti del servizio ed i professionisti sanitari a muoversi in un ambito nazionale ed internazionale; la necessità di ridurre il «carico malattia»[5]; l'esigenza di limitare il numero degli infortuni e delle malattie professionali.

Da tale prospettiva l'informatizzazione del servizio sanitario viene vista come una sorta di ricetta utile ad innalzare la qualità del servizio offerto da un lato, e ad abbassare i costi di erogazione delle prestazioni dall'altro[6].

---

[5] Il c.d. carico malattia è un indicatore della salute di una popolazione, che quantifica l'impatto globale delle malattie in termini di mortalità e di invalidità, nonché i costi connessi.

[6] L'informatizzazione, specialmente in ambito pubblico, è stata spesso concepita come una forma di risparmio economico più che come un cambiamento tecnico-organizzativo, con un determinante impatto sulle modalità stesse di esercizio della professione medica. Questo è un problema comune nel contesto del c.d. *e-government*, cioè dell'utilizzo delle tecnologie digitali da parte della pubblica amministrazione. I commentatori evidenziano come il cambiamento tecnologico debba necessariamente determinare un mutamento anche nella stessa struttura organizzativa, in special modo con riferimento ai problemi di privacy e di sicurezza che lo strumento informatico presenta. Come approfondimento sul tema v. P. GUARDA, F. MASSACCI, N. ZANNONE, *E-Government and on-line services: Security and Legal Patterns*, in F. CORRADINI, A. POLZONETTI (a cura di), *MeTTeG07. Proceedings of the 1st International Conference on Methodologies, Technologies and Tools Enabling e-Government*, Camerino, Italy, 27-28 September 2007, 29, dove si analizza il problema dalla peculiare prospettiva dell'implementazione di un sistema di autenticazione per un portale della pubblica amministrazione. Più in generale sull'*e-government* v. M. BOMBARDELLI, *Amministrazione digitale*, in *Il diritto-Encicl. giur*., Milano, 2007, vol. I, 382; F. MERLONI, *Introduzione all'@Government. Pubbliche amministrazioni e società*

Il fenomeno della digitalizzazione delle informazioni, tratto tipico dell'era digitale, determina, dunque, in ambito medico-sanitario la nascita di nuove forme di interazione che si estrinsecano sia, come sopra accennato, da un punto di vista professionale-organizzativo, che, variabile ancora più importante, da un punto di vista socio-culturale[7]. L'impatto delle tecnologie digitali sul mondo sanitario cambia i paradigmi stessi sui quali si basano le regole di responsabilità. L'*e-health* rappresenta, infatti, l'essenza di un nuovo modo di pensare degli operatori sanitari: esso deve tradursi in un approccio teorico innovativo ed in nuove modalità operative volte a migliorare l'erogazione dell'assistenza sanitaria al paziente ed a risolvere eventuali sacche di inefficienza[8].

1.2 Medicina ed Information Technology

La nostra società è caratterizzata da flussi di informazioni. Tutto ciò che conosciamo, ogni tipo di interazione, ogni ambito in cui si svolge la nostra esistenza è connotato da informazioni che vengono scambiate, aggregate, rielaborate, e che, in tal modo, mostrano aspetti sempre nuovi del nostro vivere sociale.

---

dell'informazione, Torino, 2005; G. VESPERTINI (a cura di), *L'e-Government*, Milano, 2004; F. SARZANA DI S. IPPOLITO (a cura di), *E-Government. Profili teorici ed applicazioni pratiche del governo digitale*, Piacenza, 2003; M. BOMBARDELLI, *Informatica pubblica, e-government e sviluppo sostenibile*, in *Riv. it. dir. pubbl. comunitario*, 2002, 991.

[7] Sulle caratteristiche del diritto dell'era digitale v. G. PASCUZZI, *Il diritto dell'era digitale*, III ed., Bologna, 2010, 267-309.

[8] BUCCOLIERO, CACCIA, NASI, *e-he@lth. Percorsi di implementazione dei sistemi informativi in sanità*, cit., 3, dove, in nota, si riporta un'osservazione di G. EYSENBACH, *What is e-health? [editorial]*, in *Journal of Medical Internet Research*, vol. 3, n. 2, 2001, e(20): «[…] the term characterizes not only a technical development, but also a state-of-mind, a way of thinking, an attitude, and a commitment for networked, global thinking, to improve health care […]».

La medicina stessa è una scienza basata sulle informazioni[9]. Il lavoro del medico, da Ippocrate l'Asclepiade ad oggi, è sempre stato caratterizzato dallo studio empirico dei sintomi delle malattie, per poi addivenire ad una cura (più o meno) efficace. Per far questo, i seguaci del fondatore della medicina hanno, sin dagli inizi, raccolto indizi e notizie su quei mali che i pazienti lamentavano. Il fenomeno che produce ciò che oggi definiremmo il flusso informativo che va dal paziente verso il medico è dunque nato con la medicina stessa. Ma la medicina è anche informazione sul paziente. I dati così raccolti – ed annotati allora su pergamene, ora su file elettronici – sono aggregati e catalogati in base alle differenti categorie mediche, con lo scopo di conservare e mettere a frutto l'esperienza empirica al fine di trovare la cura migliore. Si può, dunque, convenire con chi ha osservato che, per certi versi, l'informazione coincide con la cura stessa[10].

Lo sviluppo tecnologico non ha fatto altro che fornire al professionista medico strumenti nuovi per rendere sempre più oggettivo ed affidabile il flusso di informazioni che proveniva dal paziente. Le moderne tecniche di diagnostica, giovandosi di strumenti via via più sofisticati, hanno colmato il *deficit* informazionale tra medico e paziente, fornendo al primo dati sempre più nitidi, precisi e soprattutto oggettivi sulla sintomatologia descritta dal secondo[11].

La massa di informazioni, intese sia in senso soggettivo (derivanti dal paziente) che oggettivo (derivanti da indagini strumentali),

[9] Come approfondimento del rapporto tra medicina ed informazione, si v. il contributo di IZZO, *Medicina e diritto nell'era digitale*, cit., 807, dove vengono sviscerate, in tempi potremmo dire non sospetti, quelle che sarebbero state poi le linee evolutive di una professione medica che sempre più si serviva della scienza informatica per migliorare le proprie capacità di cura.

[10] Cfr. *ibidem*, 807 ss.

[11] Cfr. H.G. GADAMER, *Dove si nasconde la salute*, Milano, 1994, 135 ss.; J.G. MAZOUÈ, *Diagnosis Without Doctors*, 15 *Med. & Phi*. 559 (1990); R.A. MILLER, *Why the Standard View is Standard: People, not Machines, Understand Patients' Problems*, 15 *J. Med., & Phi.* 581 (1990).

aggregata, archiviata e catalogata diviene poi «esperienza» per la comunità scientifica[12]. Si tratta di un aspetto su cui fermare l'attenzione. È l'aggregazione delle informazioni ad aumentare in maniera sempre più incisiva le possibilità di individuare il corretto processo curativo, secondo una linea evolutiva fatta spesso di insuccessi, ma sicuramente anche di piccoli passi verso il miglioramento delle condizioni di salute degli esseri umani. Ed è proprio questo risvolto, legato all'aggregazione di dati ed alla loro disponibilità, che sta alla base dei moderni progetti di FSE e più in generale di sanità elettronica. Il rapido accesso alle informazioni dei pazienti, eliminando il rischio legato all'oblio delle stesse, rappresenta oggi più che mai una caratteristica fondamentale dello sviluppo dei sistemi sanitari moderni.

Il flusso informativo non è unidirezionale, ma bidirezionale, o, potremmo anzi meglio dire, circolare. Le informazioni, infatti, che provengono dal paziente, giungono al professionista sanitario, vengono da questi catalogate, rielaborate ed aggregate per ritornare, infine, al paziente sotto forma di cura, cioè di un percorso terapeutico proposto a quest'ultimo nella forma di una mappa di prescrizioni e procedure che egli deve conoscere ed applicare. Si può a ragione sostenere che la più parte delle attività volte a mantenere e ristabilire la salute del paziente si estrinsechino mediante l'erogazione di informazioni al paziente stesso.

L'informazione sull'attività medica determina, a sua volta, nuove conseguenze, con un notevole impatto sul mondo giuridico. Essa diventa, infatti, essenziale per garantire la piena realizzazione dei diritti del paziente. Ciò si evidenzia soprattutto nel caso in cui la valutazione

[12] In IZZO, *Medicina e diritto nell'era digitale*, cit., 808 si legge: «divenuta *caso*, l'informazione sul paziente si oggettivizza, viene aggregata e validata secondo canoni epidemiologici e scientifici, per diventare nuova conoscenza da impiegare a fini diagnostici e terapeutici». V. anche A. ZANUTTO, *Innovazione tecnologica e apprendimento organizzativo: la telemedicina ed il sapere medico*, Milano, 2008; W.F. BYNUM, *Science and the Practice of Medicine in the Nineteenth Century*, Cambridge, 1994, 191.

dell'operato del medico esca dall'ambito dell'ospedale ed arrivi nelle aule dei tribunali. Nel contesto giudiziario l'informazione medica deve presentarsi in forme documentali atte a soddisfare le tipiche esigenze di certezza ed autenticità richieste dal diritto[13]. Ritroveremo anche nell'ambiente digitale l'esigenza di garantire l'efficacia giuridica ai nuovi strumenti informatici attraverso i quali si estrinseca l'attività medica del terzo millennio.

Occorre, inoltre, affrontare il tema delle informazioni sanitarie dal punto di vista della tutela dei dati personali. L'art. 4, co. 1, lett. d, del Codice Privacy definisce i c.d. «dati sensibili» come:

> i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

Per il trattamento di tali informazioni è stata prevista una disciplina maggiormente protettiva proprio alla luce delle possibili forme di discriminazione che da esso potrebbero derivare[14].

---

[13] V. Izzo, *Medicina e diritto nell'era digitale*, cit., 809; v. anche con specifico riferimento agli *Electronic Health Record* il saggio di S. HOFFMAN, A. PODGURSKI, *E-Health Hazards: Provider Liability and Electronic Health Record Systems*, 24 *Berkeley Tech. L.J.* 1523 (2009), nelle cui conclusioni si legge: «EHR systems cannot remain unregulated and largely unscrutinized. Only with appropriate interventions will they become a blessing rather than a curse for health care professionals and patients».

[14] Con riferimento al trattamento dei dati inerenti lo stato di salute nel sistema giuridico italiano, v. per approfondimenti G. FINOCCHIARO, *Il trattamento dei dati sanitari: alcune riflessioni critiche a dieci anni dall'entrata in vigore del Codice in materia di protezione dei dati personali*, in G.F. FERRARI (a cura di), *La legge sulla privacy dieci anni dopo*, Milano, 2008, 207-220; S. VICIANI, *Brevi osservazioni sul trattamento dei dati interenti la salute e la vita sessuale in ambito sanitario*, in *Riv. crit. dir. priv*., 2007, 315; F. CAGGIA, *Il trattamento dei dati sulla salute, con particolare riferimento all'ambito sanitario*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *Il codice del trattamento dei dati personali*, Torino, 2007, 405; S. CORONATO, *La tutela della*

Essendo, quindi, i dati inerenti lo stato di salute (*rectius*, i dati sanitari) considerati sensibili per antonomasia, il loro trattamento rientra nell'ambito di applicazione della più stringente disciplina prevista dal Codice Privacy[15].

Tralasciando per ora l'analisi delle numerose questioni che riguardano i dati sanitari – il consenso necessario alla loro raccolta, l'individuazione delle informazioni che rientrano in tale categoria,

---

privacy in ospedale, in *Ragiusan*, 2006, fasc. 265/266, 6; A. FABBRI, F. MARAN, *Diritto di accesso e diritto di riservatezza: convivenza possibile?*, *id.*, 2006, fasc. 265/266, 10; ID., *Il codice per la protezione dei dati personali e l'attività socio-sanitaria integrata*, *id.*, 2005, fasc. 257/258, 19; F. MASCHIO, *Il trattamento dei dati sanitari. Regole generali e particolari trattamenti per finalità di rilevante interesse pubblico*, *id.*, 2005, fasc. 257/258, 6; E. VARANI, *Il diritto di accesso ai documenti amministrativi contenenti dati sanitari*, in *Foro amm. – T.A.R.*, 2005, 929; ID., *Diritto alla privacy e trattamento dei dati sensibili in ambito sanitario: dalla Carte dei diritti fondamentali dell'Unione europea al d.lgs.. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali"*, in *Giur. it.*, 2005, 1769; T. MINELLA, *Privacy e sanità*, in *Ragiusan*, 2005, fasc. 259/260, 22; R. ACCIAI, *La tutela della privacy ed il s.s.n.*, in *Ragiusan*, 2003, fasc. 225/226, 20; F. DI CIOMMO, *Il trattamento dei dati sanitari tra interessi individuali e collettivi*, in *Danno e resp.*, 2002, 121; C. SARZANA DI S. IPPOLITO, *La protezione dei dati personali nel campo sanitario: problemi giuridici e tecnologici*, in *Dir. informazione e informatica*, 1999, 29; P. DE CAMELIS, *Privacy e potere informatico – Cenni al trattamento dei dati inerenti la salute*, in *Rass. amm. sanità*, 1998, 4; A. CIATTI, *La protezione dei dati idonei a rivelare lo stato di salute nella legge n. 675/1996*, in *Contratto e impr./Europa*, 1998, 368. Un saggio un po' datato ma ancora estremamente interessante sulla privacy dei dati sanitari da una prospettiva di analisi economica del diritto è costituito da P.M. SCHWARTZ, *Privacy and the Economics of Health Care Information*, 76 *Tex. L. Rev*. 1 (1997).

[15] La categoria dei «dati sanitari» non riguarda solo le informazioni relative allo stato di salute diagnosticato ed attuale, bensì deve ricomprendere anche tutte le informazioni relative allo stato fisico, psichico e le relazioni dell'individuo: v. in tal senso J. MONDUCCI, G. PASETTI, *Il trattamento dei dati sanitari e genetici (Parte II – Titolo V)*, in J. MONDUCCI, G. SARTOR (a cura di), *Il codice in materia di protezione dei dati personali. Commentario sistematico al d.lgs. 30 giugno 2003, n. 196*, Padova, 2004, 255, 256-257. V. anche sull'argomento F. DI CIOMMO, *La privacy sanitaria*, in PARDOLESI (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, cit., 239; CAGGIA, *Il trattamento dei dati sulla salute, con particolare riferimento all'ambito sanitario*, cit., 407-410.

l'individuazione dei titolari del trattamento, ecc. – basti qui rilevare come tutto ciò finisca con l'addossare agli operatori in ambito medico nuove responsabilità rispetto alle garanzie dei diritti del paziente sorvegliate dalla normativa sulla protezione dei dati personali. Sorgono, dunque, nuove problematiche giuridiche legate all'ideazione ed alla predisposizione di una struttura informatica capace di fornire al cittadino la possibilità di accedere al proprio FSE all'interno dei vari contesti in cui può esprimersi il suo rapporto con il sistema sanitario (medico di base, pediatra, distretto, ospedale, proprio computer connesso ad Internet).

1.3 Premesse metodologiche e linee evolutive dei servizi informativi in sanità

I notevoli progressi tecnologici nei settori delle telecomunicazioni, dell'informatica e delle tecnologie biomediche e diagnostiche hanno determinato in campo sanitario una positiva interazione tra questi ambiti del sapere (tecnologico) umano, portando di conseguenza ad un sensibile miglioramento in termini di riduzione dei tempi, di qualità dei servizi e delle prestazioni sanitarie da un lato, e ad una più efficiente utilizzazione delle risorse dall'altro[16].

Si parla, allora, di «telemedicina»[17]. Con tale neologismo si intende l'utilizzo di tecnologie informatiche, di sistemi informativi e di

[16] Cfr. G. CANGELOSI, *I servizi pubblici sanitari: prospettive e problematiche della telemedicina*, in *Dir. famiglia*, 2007, 431. Più in particolare, uno studio sul rapporto tra il mondo della sanità e le reti di telecomunicazione con approccio caratterizzato dalle scienze cognitive in M. MORUZZI, *Internet e Sanità. Organizzazioni e management al tempo della rete*, Milano, 2008.

[17] Per un approfondimento a carattere sociologico, v. S. GHERARDI, A. STRATI (a cura di), *La telemedicina. Fra tecnologia e organizzazione*, Roma, 2004, in part. 2 e ss. Per ulteriori approfondimenti v. F. ABET, *Il ruolo delle tecnologie per una sanità moderna: la telemedicina*, in *Informatica & Documentazione*, 2007, 51; A. NARDONE, M. TRIASSI, *Profili organizzativi e giuridici della telemedicina nel quadro delle risorse tecnologiche in sanità*, in *Sanità pubblica e privata*, 2003, 2; A. ROSSI MORI, F. CONSORTI, R. NARDI, F.L. RICCI, *Un quadro di riferimento sulle tecnologie*

telecomunicazione nel campo della medicina, al fine di erogare una pluralità di servizi: assistenza sanitaria, diagnosi, consulti e terapie, trasferimento di dati sanitari, didattica, ricerca, sistemi informatici, ecc.[18].

L'introduzione delle *Information Communication Technology* (ICT) in ambito sanitario ha conosciuto diverse fasi caratterizzate dalla disponibilità – dopo la seconda guerra mondiale – di nuove tecnologie di *imaging* medica (v. ultrasuoni) e di trasmissione di immagini e contenuti audio[19] e dall'affermarsi, alla fine degli anni settanta, di nuove tecnologie ICT, divenute più economiche e di facile utilizzo[20].

---

dell'informazione nel settore sanitario, 2002, reperibile all'URL: <http://dns2.icar.cnr.it/cannataro/unicz/didattica/medicina/ISEI-MED-II/ModuloReti/Monografie/QuadroRiferimentoInformaticaSanitaria.pdf>; E. BRENNA, *La valutazione economica delle tecnologie in sanità con particolare riferimento all'area della telemedicina*, in *Sanità pubbl*., 2001, 89; IZZO, *Medicina e diritto nell'era digitale*, cit., 810-811.

[18] Nell'esperienza statunitense si rinviene una pioneristica definizione legislativa del fenomeno: cfr. § 2290.5 del *Business and Professions Code* dello Stato della California, aggiunto dal *Telemedicine Development Act* del 1996 «"telemedicine" means the practice of health care delivery, diagnosis, consultation, treatment, transfer of medical data, and education using interactive audio, video, or data communications. Neither a telephone conversation nor an electronic mail message between a health care practitioner and patient constitutes "telemedicine" for purposes of this section». Un altro utile riferimento ci è fornito dal legislatore francese che all'art. L6316-1 del *Code de la santé publique* così definisce la telemedicina: «la télémédecine est une forme de pratique médicale à distance utilisant les technologies de l'information et de la communication**.** Elle met en rapport, entre eux ou avec un patient, un ou plusieurs professionnels de santé, parmi lesquels figure nécessairement un professionnel médical et, le cas échéant, d'autres professionnels apportant leurs soins au patient. Elle permet d'établir un diagnostic, d'assurer, pour un patient à risque, un suivi à visée préventive ou un suivi post-thérapeutique, de requérir un avis spécialisé, de préparer une décision thérapeutique, de prescrire des produits, de prescrire ou de réaliser des prestations ou des actes, ou d'effectuer une surveillance de l'état des patients».

[19] Cfr. J. GRISBY, M.M. KAHENY, E.J. SANDBERG, R.E. SCHLENKER, P.W. SHAUGHNESSY, *Effects and Effectiveness of Telemedicine*, 17 *Health Care Financing Rev*. 115 (1995).

[20] Cfr. C. MAY, N.T. ELLIS, *When Protocols Fail: Technical Evaluation, Biomedical Knowledge, and the Social Production of 'Facts' about a Telemedicine Clinic*, in *Social Science and Medicine*, vol. 53, Issue 8, 2001, 989.

Rimanendo ad una concezione di telemedicina intesa come erogazione di servizi sanitari a distanza, si può proporre una loro classificazione basata sugli ambiti applicativi con riferimento alle specialità disciplinari della pratica medica[21]. Senza alcuna pretesa di esaustività prendiamoli in rassegna.

Un primo servizio offerto tramite la telemedicina è costituito dal «teleconsulto». In questo caso i pazienti utilizzano tecnologie di telecomunicazione per ottenere un servizio di consulenza da parte di un operatore sanitario. Tale contatto avviene da remoto con la presenza simultanea di paziente e specialista, entrambi in linea nello stesso momento.

Vi sono, poi, le «teleconferenze», quando uno o più sanitari responsabili della cura di un paziente comunicano tra loro attraverso un collegamento audio-video. Ciò accresce notevolmente le possibilità di approntare una valida cura, favorendo il confronto tra professionisti distanti fisicamente e depositari di diversi saperi e specialità.

Un altro servizio erogato è quello di *telereporting*. Con tale termine si intende la trasmissione di dati relativi ad un caso clinico da parte di un operatore sanitario verso un proprio collega specialista, al fine di sottoporgli il caso e ottenere un parere specialistico.

Infine, in questa carrellata di precisazioni terminologiche, occorre menzionare il «telemonitoraggio», il quale consiste nella raccolta di dati sul paziente, inviati successivamente ad un centro remoto (si veda ad esempio il telemonitoraggio dei pazienti affetti da scompenso cardiaco o in acuzie). Questo tipo di servizi può essere direttamente collegato ai sistemi di FSE, i quali, infatti, sono caratterizzati da

[21] Si prenda a riferimento GHERARDI, STRATI (a cura di), *La telemedicina*, cit., 22 ss. Altri propongono una diversa categorizzazione: si v., ad es., P. TAYLOR, *A Survey of Research in Telemedicine*, in *Telemedicine Services. Journal of Telemedicine and Telecare*, 4, 2, 1998, 223, il quale presenta una suddivisione dei servizi di telemedicina in: servizi di trattamento, servizi diagnostici e servizi informativi ed educativi.

un'alimentazione informazionale proveniente da più fonti: professionisti sanitari, pazienti, strumenti informatizzati di autorilevazione, ecc.

Negli anni novanta si registra la diffusione capillare delle tecnologie informatiche e soprattutto l'avvento di Internet, il quale ha determinato uno sconvolgimento tale che la stessa categoria «telemedicina» – forse appropriata nell'era del c.d. Internet 1.0 – è divenuta insufficiente a designare le nuove molteplici modalità di interazione tra assistiti e curanti. Si è cominciato, così, a fare riferimento a nozioni a carattere più generale, quali *tele-health*, *e-health* o «cybermedicina», «sanità elettronica», le quali dimostrano un ampliamento delle possibilità offerte dallo sviluppo tecnologico verso orizzonti ancora non completamente esplorati[22].

Tuttavia, l'impatto di questo graduale cambiamento tecnologico non sempre è stato ben governato da parte degli attori dei servizi sanitari nazionali e locali. L'adozione di strumenti informatici da parte delle aziende sanitarie è avvenuta non di rado in assenza di una chiara visione d'insieme e senza tenere in debito conto le esigenze di integrazione tra i sistemi sia all'interno che all'esterno della struttura di riferimento[23]. Anzi, sovente si è assistito ad interventi caratterizzati da una logica

[22] Nel saggio di IZZO, *Medicina e diritto nell'era digitale*, cit., 811-817 troviamo un'attenta catalogazione dei problemi giuridici di cui telemedicina e cybermedicina si caratterizzano. In generale sulla sanità elettronica (*e-health*) in dottrina v. R. LATIFI (a cura di), *Current principles and practices of telemedicine and e-health*, Amsterdam, 2008; B.J. CRIGGER, *e-Medicine: Policy to Shape the Future of Health Care*, 36 *The Hastings Center Report* 12 (2006); N.P. TERRY, *A Medical Ghost in the E-Health Machine*, 14 *Health Matrix* 225-29 (2004); A. SINHA, *An Overview of Telemedicine: The Virtual Gaze of Health Care in the Next Century*, 14 *Medical Anthropology Quarterly. New Series* 291 (2000).

[23] Per un'approfondita ricognizione dei processi evolutivi dei sistemi informativi nelle aziende sanitarie, v. C. CACCIA, *Management dei sistemi informativi in sanità*, Milano, 2008; BUCCOLIERO, CACCIA, NASI, e-*he@lth*, cit.; M. MORUZZI, *Fascicolo sanitario elettronico personale e reti e-Health. Appunti per un'analisi della sanità di Internet*, in *Salute e società*, 2008, fasc. 3, 1; A. MACCARI, G. ROMIGI, *Le basi concettuali e pratiche di un Sistema Informativo Sanitario*, Santarcangelo di Romagna, 2009.

dell'aggiunta, della sedimentazione, degli adattamenti di parti dei sistemi informativi, invece che da un chiaro e lungimirante approccio attento alla riprogettazione periodica dell'esistente da un punto di vista informatico e, soprattutto, organizzativo.

Nelle aziende sanitarie spesso si è venuto a determinare uno scenario di resistenza all'innovazione. Questo è avvenuto a causa di diversi fattori, quali: la scarsa volontà e partecipazione che caratterizza l'operato delle direzioni sanitarie ad impegnarsi in progetti caratterizzati da alti costi, alto rischio strategico ed elevata complessità; l'incerto clima istituzionale e la ridotta capacità d'investimento legata alla scarsità di risorse a disposizione del servizio sanitario nazionale (SSN); la debole attitudine all'investimento in ricerca e sviluppo, che purtroppo contraddistingue più in generale la storia del rapporto tra ricerca scientifica e mondo del lavoro[24].

Ultimamente sembra spirare un vento di cambiamento: grazie alla oramai capillare diffusione delle ICT ed all'acquisita consapevolezza dell'importanza della gestione e trattamento dei dati sanitari, si assiste ad una rinnovata sensibilità verso un uso integrato delle informazioni, non solo a livello aziendale, ma anche su scala regionale, nazionale ed europea nella prospettiva sia di garantire l'erogazione di una migliore assistenza sanitaria sia di focalizzare l'attenzione su esigenze legate a finalità di ricerca, statistiche o di studi epidemiologici. Nell'ambito di questo cambiamento si ritrova la posizione in via di consolidamento del paziente all'interno del sistema, il quale, in tal modo, assume un ruolo attivo nei processi di cura dei quali è il destinatario.

È auspicabile che tale vento di cambiamento, sicuramente avvertito dai protagonisti della sanità elettronica, possa condizionare veramente in profondità le logiche applicative dei progetti che si stanno approntando a livello regionale e provinciale.

[24] Cfr. BUCCOLIERO, CACCIA, NASI, *e-he@lth*, cit., 85.

2. Il panorama normativo della sanità elettronica

Negli ultimi anni si è verificata una notevole evoluzione dei sistemi di assistenza sanitaria, dovuta anche al rapido sviluppo di nuove tecnologie che stanno rivoluzionando le modalità di promozione della salute, come pure quelle di predizione, prevenzione e trattamento delle malattie.

Un sondaggio pubblicato il 25 aprile 2008 dalla Commissione europea sull'utilizzo di servizi elettronici per l'assistenza sanitaria (*eHealth*) rivela che l'87% dei medici generici europei usa il computer (l'Italia è all'86%) ed il 48% dispone di una connessione a banda larga (in Italia il 49%)[25]. Il 69% utilizza Internet (la percentuale sale al 71% in Italia) ed il 66% si serve del computer durante le visite. In Italia, poi, oltre il 25% impiega la posta elettronica per scambiare informazioni con altri medici, quando la media europea non supera il 20%. In Europa (e anche in questo caso l'Italia è nella media) i dati amministrativi dei pazienti vengono conservati in forma elettronica nell'80% degli studi medici; il 92% di questi è solito archiviare elettronicamente anche i dati relativi a diagnosi e terapie ed il 35% conserva in formato elettronico le radiografie. Il sondaggio evidenzia anche le aree che si prestano a ulteriori progressi, come per quanto riguarda le ricette elettroniche, che sono utilizzate solo dal 6% dei medici generici dell'UE (in Italia siamo appena all'1%).

A fronte di questi fenomeni in fieri che stanno determinando profonde trasformazioni strutturali e organizzative nel sistema sanitario, i governi nazionali e regionali dei Paesi tecnologicamente avanzati hanno dato vita a piani strategici per traghettare tale transizione e

[25] V. COMMISSIONE EUROPEA, *Un sondaggio tasta il polso della sanità elettronica in Europa e prescrive ai medici un più ampio uso delle TIC*, Bruxelles, 25 aprile 2008, in Rete: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/08/641&format=HTML&aged=0&language=IT&guiLanguage=e>.

favorire la diffusione delle ICT in ambito medico[26].

La Comunità europea ha fatto la sua parte e da diversi anni finanzia in vario modo simili progetti[27].

Per riferirsi solo all'ultimo decennio, il 23 settembre del 2002 si approvava con la Decisione n. 1786/2002/Ce del Parlamento europeo e del Consiglio un «Programma d'azione comunitaria in materia di salute pubblica (2003-2008)». Questo programma, oltre ai tradizionali obiettivi focalizzati sull'informazione e la conoscenza della sanità, sulla capacità di reazione rapida e coordinata della Comunità e sulla prevenzione delle malattie, prevedeva la possibilità di utilizzare le tecnologie informatiche e telematiche al fine di potenziare la qualità dell'assistenza sanitaria in tutta Europa.

Nel 2004 la Commissione europea adottava un piano d'azione sulla sanità elettronica: «Sanità elettronica – migliorare l'assistenza sanitaria dei cittadini europei: piano d'azione per uno spazio europeo della sanità elettronica» (chiamato anche *Action Plan eHealth* 2004), con cui veniva prospettata la possibilità d'impiegare le tecnologie informatiche e telematiche (ICT) al fine di migliorare la qualità dell'assistenza sanitaria in tutta Europa, mantenendo i costi stabili o riducendoli, abbreviando, così, i tempi di attesa e diminuendo i margini d'errore[28]. Con il piano d'azione a livello comunitario si perseguiva l'obiettivo della creazione di uno «spazio europeo della sanità elettronica»: a tal fine, venivano indicate le misure concrete per la sua realizzazione, puntando sull'applicazione delle tecnologie informatiche e telematiche per le ricette, le cartelle mediche, l'identificazione dei

[26] Cfr. CANGELOSI, *I servizi pubblici sanitari*, cit., 448 ss.

[27] Per una descrizione del profilo storico della strategia comunitaria in materia di salute, v. SARTORI, *La tutela della salute pubblica nell'Unione europea*, cit., 65-73.

[28] Comunicazione della Commissione al Consiglio, al Parlamento europeo, al Comitato economico e sociale europeo e al Comitato delle regioni, del 30 aprile 2004, «Sanità elettronica - migliorare l'assistenza sanitaria dei cittadini europei: piano d'azione per uno spazio europeo della sanità elettronica», in Rete: <http://europa.eu/legislation_summaries/public_health/european_health_strategy/l24226f_it.htm>.

pazienti e le tessere sanitarie, attraverso una più rapida installazione di reti a banda larga destinate ai sistemi sanitari.

Inoltre, uno dei tre pilastri dell'iniziativa «i2010 – Una società europea dell'informazione per la crescita e l'occupazione»[29] consiste nella promozione dell'«inclusione, del miglioramento dei servizi pubblici e della qualità di vita» attraverso le tecnologie dell'informazione e delle comunicazioni (TIC). A tale scopo, è stata ideata un'iniziativa faro sulle TIC che ha portato al varo del portale dell'Unione europea sulla salute pubblica[30].

Si segnalano, poi, una serie di raccomandazioni e comunicazioni della Commissione europea volte a favorire l'implementazione e lo sviluppo della sanità elettronica: il «Libro Bianco» della Commissione «Un impegno comune per la salute: Approccio strategico dell'UE per il periodo 2008-2013», Bruxelles, 23 ottobre 2007; la Raccomandazione della Commissione, del 2 luglio 2008, sull'interoperabilità transfrontaliera dei sistemi di cartelle cliniche elettroniche (COM(2008) 3282); la Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni del 4 novembre 2008 sulla telemedicina a beneficio dei pazienti, dei sistemi sanitari e della società (COM(2008) 689).

Infine, occorre almeno menzionare il progetto epSOS (*Smart Open Services for European Patients*) che ha preso avvio nel luglio del 2008 e mira a realizzare un servizio elettronico di scambio di dati sanitari in ambito europeo, nel rispetto del quadro normativo e dei sistemi informativi esistenti nei Paesi che partecipano all'iniziativa. Esso riuni-

[29] Comunicazione della Commissione al Consiglio, al Parlamento europeo, al Comitato economico e sociale europeo e al Comitato delle regioni, del 1° giugno 2005, intitolata «i2010 – Una società europea dell'informazione per la crescita e l'occupazione», in Rete: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0229:FIN:IT:PDF>.

[30] V. il portale dell'Unione europea sulla salute pubblica: <http://ec.europa.eu/ health-eu/index_it.htm>.

sce dodici Paesi dell'Unione europea rappresentati da pubbliche amministrazioni (Ministeri della Sanità a livello nazionale e regionale), centri di competenza nazionali e imprese. L'obiettivo principale del progetto epSOS è realizzare una soluzione pratica che consenta, sotto il profilo tecnico, lo scambio sicuro di dati personali tra i diversi sistemi nazionali di sanità digitale, per testare le soluzioni realizzate in un quadro operativo di siti pilota[31].

Per quanto concerne il contesto italiano, il sistema della sanità elettronica risulta caratterizzato da un ambito strategico nazionale e da diversi rilevanti interventi in ambito locale.

Occorre anzitutto ricordare il «Piano sanitario nazionale 2003-2005», con il quale il governo italiano individuava gli obiettivi generali di salute per l'Italia, alla luce dei cambiamenti del panorama sociale e politico nazionale, avendo a riferimento l'esigenza fondamentale di garantire ai cittadini la tutela della salute, la sicurezza sociale, l'equità del sistema sanitario, la sua qualità e trasparenza. All'interno di queste iniziative il patrimonio costituito dalle informazioni sulle condizioni sanitarie del cittadino, perno su cui si muove tutta la struttura medico-ospedaliera volta a migliorare i processi di cura e di assistenza del paziente stesso, diviene un elemento strategico al fine di supportare la modernizzazione del SSN.

In questo contesto, nell'ottobre del 2004 la Presidenza del Consiglio dei Ministri attivava uno strumento organizzativo definito «Tavolo di lavoro permanente per la sanità elettronica» (d'ora in avanti: TSE) al fine di coordinare e sostenere l'attuazione del «Piano Sanità Elettronica»[32]. Tale progetto è nato come sede istituzionale di confronto e con-

[31] V. il sito web dedicato: «http://www.epsos.eu/epsos-home.html».

[32] Il TSE è composto dai rappresentati del Ministro per l'Innovazione e le Tecnologie, del Ministero della Salute e delle Amministrazioni Regionali e delle Province Autonome. Sul sito web dedicato è possibile reperire tutta la produzione di documenti a carattere tecnico che tale tavolo di lavoro ha prodotto: <http://www.innovazionepa.gov.

sultazione tra le Regioni, le Province autonome e l'amministrazione centrale, allo scopo di armonizzare le politiche della Sanità Elettronica e l'attuazione dei piani d'azione nazionale e regionali. Il 31 marzo 2005 il gruppo di lavoro pubblicava un documento intitolato «Una politica condivisa per la sanità elettronica» che appare di notevole interesse ai fini della nostra analisi[33]. Con esso si compiva un passo importante per la definizione di un percorso programmatico volto all'innovazione digitale nei sistemi socio-sanitari locali e si recepivano gli obiettivi strategici dell'Unione europea, espressi nel sopra citato *Action Plan eHealth* 2004, e gli obiettivi del vecchio «Piano sanitario nazionale 2003-2005».

In esito a tali sforzi è stato emanato il «Piano industriale per l'Innovazione della P.A.», presentato a Roma il 2 ottobre 2008, che, per quanto concerne la sanità elettronica, individua cinque grandi aree di intervento: connettere in rete tutti i medici di base entro giugno 2010; realizzare il FSE entro giugno 2009; sviluppare un sistema per i Certificati di malattia digitali entro dicembre 2009 e per le Ricette digitali (in Lombardia, Emilia Romagna, Veneto, Friuli Venezia Giulia) entro giugno 2009; realizzare un sistema sovra-regionale (Umbria, Emilia Romagna, Veneto, Marche e Provincia autonoma di Trento) per le prenotazioni *on-line* entro dicembre 2009.

Infine, il «Piano di e-government 2012» realizzato dal Ministero per la Pubblica Amministrazione e l'Innovazione definisce un insieme di progetti di innovazione digitale volti a modernizzare e a rendere più efficiente e trasparente la pubblica amministrazione[34]. In particolare, esso menziona tra gli «obiettivi» da raggiungere un punto esplicitamente dedicato alla salute: vi si afferma che entro il 2012 saranno semplificati e digitalizzati i servizi elementari (prescrizioni e certificati di

---

it/i-dipartimenti/digitalizzazione-e-innovazione-tecnologica/attivita/tse/il-tavolo-permanente-per-la-sanita-elettronica-delle-regioni-e-delle-province-autonome-tse-.aspx>.

[33] In Rete: <http://www.innovazionepa.gov.it/media/566294/tse-politica%20 condivisa%20per%20la%20sanit%20elettronica.pdf>.

[34] V. il sito web dedicato: <http://www.e2012.gov.it/egov2012/>.

malattia digitali, sistemi di prenotazione *on-line*) e verranno create le infrastrutture per un'erogazione di servizi sanitari sempre più vicini alle esigenze dei cittadini (v. FSE), al fine di migliorare il rapporto costo-qualità dei servizi e di limitare sprechi ed inefficienze.

Da ultimo, è stato istituito un Tavolo interistituzionale per il FSE, cui partecipano, sotto il coordinamento del Ministero della Salute, oltre ad esperti interni ed esterni del Ministero, rappresentanti delle Regioni designati dalla Commissione salute (Lombardia, Emilia-Romagna, Toscana), del Dipartimento per la digitalizzazione della pubblica amministrazione e l'innovazione tecnologica della Presidenza del Consiglio dei Ministri, dell'ente per la digitalizzazione della Pubblica amministrazione (DigitPa) e del Garante per la protezione dei dati personali (d'ora in avanti: Garante Privacy), che interviene in qualità di osservatore. Il Tavolo di lavoro si propone l'obiettivo di individuare le caratteristiche salienti del FSE e di predisporre una cornice normativa unitaria[35]. Dopo la preliminare attività svolta di ricognizione ed analisi della normativa vigente, è stato individuato nelle finalità di cura, e nelle correlate attività amministrative, l'ambito di istituzione del FSE; si è passati, così, a sviluppare un modello di riferimento i cui risultati finali sono stati descritti nelle «Linee guida sul fascicolo sanitario elettronico» approvate nell'ambito della Conferenza Stato-Regioni il 10 febbraio 2011[36].

Alla luce della tendenza in atto il ruolo del cittadino-paziente diviene un valore centrale, come sottolinea il già menzionato Libro Bianco «Un impegno comune per la salute: Approccio strategico dell'UE per il periodo 2008-2013». L'assistenza sanitaria è sempre più orientata verso il paziente, il quale sta diventando soggetto attivo e non

[35] Il Tavolo interistituzionale ha come finalità quelle di: predisporre una cornice normativa unitaria, individuare le caratteristiche di fondo dei sistemi FSE, definire correttamente il *patient summary* e predisporre uno schema di provvedimento attuativo.

[36] Il documento è disponibile in Rete: <http://www.salute.gov.it/imgs/C_17_pubblicazioni_1465_allegato.pdf>.

più semplice oggetto di cure[37]. Egli deve poter partecipare al processo decisionale ed acquisire le competenze necessarie al suo benessere, tra le quali la cosiddetta «alfabetizzazione sanitaria». Non casualmente anche il nostro «Piano Sanitario Nazionale 2006-08» individuava, come obiettivo fondamentale, quello di

> favorire le varie forme di partecipazione del cittadino, in particolare attraverso il coinvolgimento dei pazienti e delle associazioni dei familiari.

3. Architetture informatiche e gestione dei dati sanitari

3.1 Evoluzione dei modelli di gestione informatizzata dei dati sanitari

Nella letteratura della scienza informatica la nozione italiana di FSE può essere resa, in prima approssimazione, con l'espressione anglosassone *Electronic Health Record* (d'ora in avanti EHR). In realtà con tale categoria ci si riferisce ad altre esperienze e concetti che finiscono per rendere confuso il quadro dogmatico-definitorio della materia.

Il crescente interesse sugli EHR si è sviluppato parallelamente all'aumento del numero di tentativi di definirli. Nel corso degli anni si è utilizzata, infatti, l'espressione EHR con riferimento a diversi modelli: *Electronic Medical Record*, *Electronic Patient Record*, *Computer-stored Patient Record*, *Ambulatory Medical Record*, *Computer-based medical record*[38].

---

[37] Si v. E.V. WILSON (a cura di), *Patient-centered e-health*, Hershey, Pa., New York, N.Y., 2009.

[38] Cfr. M.K. AMATAYAKUL, *Electronic Health Records. A Practical Guide for Professionals and Organizations*, Chicago, 2009, 1-28; J.H. CARTER, *Electronic Health Records. A Guide for Clinicians and Administrators*, II ed., Philadelphia, 2008, 5-7; N.P. TERRY, L.P. FRANCIS, *Ensuring the Privacy and Confidentiality of Electronic*

Per far chiarezza sul punto, si procederà alla descrizione dell'evoluzione che i sistemi informatizzati di gestione dei dati sanitari hanno conosciuto in modo da poter dare una precisa definizione di termini e concetti che si sono poi affermati e che caratterizzano ora il contesto operativo del tema oggetto di analisi.

Seguiremo nell'esposizione lo schema evolutivo delle architetture informatiche proposto dal *Medical Record Institute*, il quale si basa sulla distinzione tra modelli di aggregazione dei dati, finalità, complessità architetturale e *focus*[39].

Il primo modello, che si diffonde nei primi anni novanta, si definisce *Automated Medical Record* (AMR) ed è caratterizzato da un elevato livello di strutturazione dei dati elaborati ed archiviati, con lo scopo di riuscire a supportare l'attività di singole categorie di utenti (medici e specializzandi). Le architetture sono concepite in modo tale da poter fornire un utile supporto alle esigenze specifiche di un determinato reparto (ad esempio, un database relativo alla leucemia in un reparto di ematologia che raccoglie informazioni derivanti da specifici esami di laboratorio). Questi tipi di sistema non intendono assolutamente sostituirsi alla cartella clinica cartacea. Generalmente si trovano su computer *stand-alone*. Sono oramai adottati in tutte le realtà sanitarie, anche se spesso non vengono considerati parte del sistema informativo.

Nella seconda metà degli anni novanta, poi, si affermano le architetture c.d. *Computerised Medical Record* (CMR). Questo modello

---

Health Records, 2007 *U. Ill. L. Rev*. 681, 686-688 (2007); P.C. TANG, C.J. MCDONALD, *Electronic health record systems,* in E.H. SHORTLIFFE, J.J. CIMINO (a cura di), *Biomedical informatics: Computer applications in health care & biomedicine,* New York, NY, 2006, 447-475; J. WALKER, E.J. BIEBER, F. RICHARDS (a cura di), *Implementing an electronic health record system*, New York, N.Y., 2006.

[39] Si riprende la linea espositiva seguita in BUCCOLIERO, CACCIA, NASI, *e-he@lth*, cit., 86-94, spec. 86-87 dove viene richiamato lo schema evolutivo delle architetture informatiche proposto da C.P. WAEGEMANN, *Status Report 2002: Electronic Health Records*, Medical Record Institute, 2002; v. anche CACCIA, *Management dei sistemi informativi in sanità*, cit., 130-146.

si basa su di un sistema di cartelle cliniche cartacee ed altri documenti digitalizzati e resi disponibili in un singolo *data repository* a cui hanno accesso i diversi professionisti sanitari che operano all'interno della struttura. Si caratterizza per la sua maggiore interoperabilità e facilità nel favorire una consultazione simultanea delle informazioni presenti nella banca dati. Per ovviare alle lungaggini dovute ai tempi di duplicazione dell'attività di registrazione dei dati, prima in modalità cartacea e poi attraverso lo strumento digitale, alcune esperienze, soprattutto all'estero, hanno visto l'implementazione di strumenti di inserimento automatico delle informazioni da parte del personale di segreteria del reparto. Il sistema presenta alcune interessanti peculiarità: garantisce un rapido accesso alle informazioni e salvaguarda la sicurezza dei dati, con riferimento all'autenticità del loro inserimento, all'identità dell'operatore ed alla marcatura temporale. Tale modello di gestione permette un aumento dell'efficienza del servizio sanitario, in termini di costi e di tempo, nel processo di ricostruzione della storia clinica del paziente. Un sistema di tal sorta permette anche di ridurre il rischio di perdita accidentale di documenti sanitari. Appare evidente come la buona riuscita di questo modello si basi su di un efficiente sistema di indicizzazione nell'inserimento dei dati che sia allo stesso tempo univoco e condiviso. Ciò comporta anche una rivalutazione e ridistribuzione dell'organizzazione dei soggetti coinvolti, alla luce dei flussi informativi così generati[40].

Un terzo livello di strutturazione dell'architettura prende il nome di *Electronic Medical Record* (EMR). Qui il punto di riferimento diventa la struttura sanitaria, all'interno della quale si riorganizza il sistema di gestione dei flussi informativi al fine di potenziare e migliorare le attività di cura. Per far ciò si costruisce un *data repository* clinico

[40] V. l'esempio virtuoso dell'Azienda ULSS n. 9 di Treviso, la quale tramite il progetto ESCAPE ha avviato la pianificazione della completa digitalizzazione dei documenti clinici ed amministrativi.

aziendale unitario all'interno del quale confluiscono tutte le informazioni cliniche prodotte nelle diverse circostanze che vedono il paziente entrare in contatto con la struttura stessa, a loro volta distribuite nei diversi applicativi informatici. Per far funzionare questo tipo di architettura, occorre costruire ed organizzare un sistema di anagrafica centralizzata, volta ad indicizzare tutti i dati relativi ai pazienti, ed un sistema di gestione del c.d. *workflow* (flusso di lavoro), atto a governare le attività sanitarie effettuate nella struttura e quelle di gestione amministrativa (quali, ad esempio, le prenotazioni degli esami specialistici).

Un quarto modello di architettura che si è cominciato ad affermare agli inizi del 2000 è il c.d. *Electronic Patient Record* (EPR) il quale individua una struttura informatica che si basa su quella appena analizzata di EMR, che però presuppone un'interazione tra strutture ed aziende sanitarie diverse, sistematicamente coinvolte nel processo diagnostico e curativo di un determinato paziente[41]. Questo tipo di architettura si basa su una visione d'insieme di molti sistemi informativi che vedono la titolarità del trattamento in capo a diverse strutture sanitarie. Generalmente si organizza in modo tale da permettere l'archiviazione e l'elaborazione solo di una limitata quantità di informazioni di rilevante interesse clinico relative ad un soggetto (*rectius*, il c.d. *patient summary*).

Il modello sicuramente più conosciuto è rappresentato dal c.d. *Electronic Health Record* (EHR). Anche tale soluzione si caratterizza per un'architettura sostanzialmente fondata su quella di EMR che risulta condivisa da parte di più professionisti che operano in strutture diverse ma facenti parte della stessa organizzazione a livello geografico (vedi un'Azienda sanitaria). Il EHR si basa su un'idea di fondo diversa e rivoluzionaria rispetto alle precedenti: il paziente non è visto solo come fulcro di un sistema che lo concepisce quale oggetto passivo del proces-

[41] V. l'esempio del *National Health Service* inglese e del CRS-SISS della Regione Lombardia.

so curativo, quanto come «primo attore» nelle decisioni che riguardano la sua salute. Tale visione concettuale si estrinseca nell'implementazione di strutture informatiche atte a trasferirgli (talvolta) la stessa responsabilità nella gestione delle informazioni cliniche che lo riguardano[42]. Possiamo, così, avere *patient record* contenute all'interno del *repository* dell'azienda sanitaria, così come aree riservate nel portale ad accesso consentito al solo paziente.

L'ultimo modello in ordine di tempo prende il nome di *Personal Health Record* (PHR). Tale sistema si connota per un approccio orientato all'archiviazione ed all'elaborazione delle sole informazioni rilevanti per il paziente. I vari dati generati dalle infrastrutture che abbiamo descritto sopra (EMR, EPR e EHR) sono qui resi integralmente disponibili al paziente, il quale solo decide la modularizzazione dei livelli di accesso ad essi. A differenza delle tradizionali piattaforme di gestione informatizzata dei dati sanitari, che privilegiano il ruolo dei gestori del servizio sanitario dedicando all'utente una posizione del tutto marginale e limitata, questo nuovo modello è caratterizzato da una struttura che elegge il paziente a baricentro del sistema di gestione delle informazioni idonee a rivelare il suo stato di salute. In questa prospettiva, ogni sua interazione con il sistema implicherà la creazione di nuovi dati. La prima rivoluzione digitale dei dati sanitari – l'introduzione, dapprima, delle tecnologie dell'informazione e, successivamente, della documentazione sanitaria elettronica (EHR) – riguardava, infatti, la di-

[42] Cfr. K.A. ROKITA, J.E. TOPPER, M.C. LAMPMAN, D.L. YOUNG, *Extending EHR access to patients*, in J. WALKER, E.J. BIEBER, F. RICHARDS (a cura di), *Implementing an electronic health record system*, New York, N.Y., 2006, 153-169, spec. 153 dove gli autori ricordano che: «Giving patients electronic access to their EHR and secure E-messaging via a patient EHR has the potential to revolutionize healthcare. With easier access to more information, patients can participate more effectively in their care […]. Both patients and practices can create more efficient ways of working together (for examples, with prescription renewals requested by the patient one evening and processed by the patient's practice the next morning). These information services can support healthcare of a quality and efficiency that is not possible without it».

gitalizzazione e la razionalizzazione dei flussi di dati. L'introduzione di una nuova rivoluzione, quale quella delle PHR, significa che i pazienti creeranno sempre più dati sanitari (o collegamenti tra questi) senza l'intermediazione di alcun «soggetto qualificato» adibito alla prestazione del servizio sanitario[43].

3.2 Definizione di Electronic Health Record

Come avremo modo di ribadire, il Garante Privacy italiano non ha fatto una chiara scelta di campo da un punto di vista tecnico-architetturale. Questi, infatti, prima di addentrarsi nella definizione particolareggiata delle sub-categorie individuate all'interno della classificazione degli strumenti atti a gestire i dati sanitari dei pazienti (FSE e *dossier*), tratta in apertura delle «Linee guida in tema di Fascicolo Sanitario Elettronico (Fse) e di *dossier* sanitario – 16 luglio 2009» (d'ora in avanti: LG FSE) de

> l'insieme dei diversi eventi clinici occorsi ad un individuo, messo in condivisione logica dai professionisti o organismi sanitari che assistono l'interessato, al fine di offrirgli un migliore processo di cura[44].

[43] Cfr. R. CUSHMAN, *Primer: Data Protection and the Personal Health Record*, Project Health Design ELSI Team, University of Miami, in Rete: <http://www.projecthealthdesign.org/media/file/primer_data_protection.pdf>; ID., *Primer: Authentication of identity (with application to PHRs/PHAs)*, in Rete: <http://www.projecthealthdesign.org/media/file/primer_authentication.pdf>; ID., *PHRs and the Next HIPAA*, 2008, in Rete: <http://www.projecthealthdesign.org/media/file/PHR_HIPAA2.pdf>; A.M. FROOMKIN, *Forced Sharing of Patient-Controlled Health Records*, Working Paper, 2008, in Rete: <http://www.projecthealthdesign.org/media/file/Forced-sharing.pdf>; ID., *The New Health Information Architecture: Coping with the Privacy Implications of the Personal Health Records Revolution*, UM ELSI Group for Project HealthDesign, 2008, in Rete: <http://www.projecthealthdesign.org/media/file/social-life-info-15.pdf>; N.P. TERRY, *Personal Health Records: Directing More Costs and Risks to Consumers*, Working Paper, August 2008, in Rete: <http://ssrn.com/abstract=1248768>.

[44] LG FSE, p. 1.5.

Non vi è qui una scelta tecnologica, bensì un'indicazione di carattere concettuale, utile nella prospettiva regolativa scandita dal bagaglio di nozioni giuridicamente rilevanti offerte dal Codice Privacy. È la condivisione logica dei dati tra organismi e professionisti sanitari in vista di un miglioramento del processo curativo che permette di dare l'*imprimatur* di FSE ad un'architettura informatica, quale che sia la modellizzazione informatica attraverso cui essa sia concepita e diventi operativa.

Il ruolo del cittadino, sebbene non richiamato nelle definizioni a carattere generale, viene ribadito a livello di inciso:

> il titolare del trattamento può, inoltre, prevedere che l'interessato possa inserire o ottenere l'inserimento – anche in appositi moduli e secondo degli standard, anche di sicurezza, definiti dal titolare – talune informazioni sanitarie (es. autovalutazioni, referti emessi da strutture sanitarie di altre regioni o Stati) o amministrativo sanitarie (es. appuntamenti medici, periodicità dei controlli prescritti) che riterrà più opportune[45].

Il sistema di FSE italiano è, pertanto, orientato verso un modello di EHR e pone in secondo piano, ma come obiettivo da raggiungere, la scelta di un'infrastruttura basata anche su un modello di PHR.

Non tralasciando il ruolo primario che, in prospettiva, il cittadino rivestirà all'interno di queste architetture, verranno di seguito analizzate ulteriori peculiarità dei sistemi di EHR, utili a meglio comprendere le modalità secondo le quali tali servizi possono essere offerti[46]. Il tutto risulterà cruciale allorquando si cercherà di conformare le architet-

[45] *Ibidem*, p. 5.9.

[46] Si prenda a riferimento AMATAYAKUL, *Electronic Health Records*, cit., 2 ss.; CARTER, *Electronic Health Records*, cit., 5 ss.; R. GARTEE, *Electronic Health Records. Understanding and Using Computerized Medical Records*, Upper Saddle River, New Jersey, 2007, 1 ss.

ture digitali ai principi ed alle regole giuridiche che connotano, in particolare, il nostro ordinamento giuridico.

Un sistema di EHR si caratterizza per tre principali funzionalità: l'integrazione di dati provenienti da diverse fonti (ospedali, professionisti sanitari, ecc.), l'acquisizione di dati presso i punti di assistenza ed il supporto all'attività clinico decisionale. Quando queste componenti sono incorporate all'interno di una singola infrastruttura ed interagiscono tra di loro in maniera armonica, possiamo considerare il risultato un EHR, appunto.

Questo fa dell'EHR un sistema, ovvero una serie di elementi interconnessi che funzionano assieme per conseguire uno scopo determinato: la cura del paziente. L'aspetto problematico dei sistemi in ambito sanitario è determinato dal fatto che i dati vengono prodotti autonomamente da parte di soggetti diversi e spesso non coordinati tra loro. L'interoperabilità gioca, quindi, un ruolo cruciale.

All'interno del sistema acquista valore l'integrazione tra informazioni di varia natura (dati clinici, dati finanziari, dati amministrativi, ecc.) che, assieme, concorrono a migliorare sensibilmente in termini di qualità, costi ed efficienza il servizio sanitario. Inoltre, il EHR non è limitato ad una singola posizione spaziale e deve invece collegare diversi e distanti punti di accesso a disposizione dei diversi utenti (pazienti) e fornitori del servizio (aziende ospedaliere, professionisti sanitari, ecc.). Esso deve essere in grado di integrare dati provenienti dagli operatori sanitari per garantire la continuità nelle cure e da sistemi PHR, al fine di porre in essere una struttura di visualizzazione longitudinale dello stato clinico e di salute di un singolo soggetto.

Da un punto di vista tecnico, le componenti di un modello di EHR sono le seguenti[47].

[47] Per un'introduzione alle caratteristiche fondamentali ed alle componenti tecniche di un sistema di EHR, v. AMATAYAKUL, *Electronic Health Records*, cit., 1-30.

Anzitutto, esso deve avere sistemi di approvvigionamento dei dati (*source system*) in grado di raccogliere le informazioni necessarie a supportare l'infrastruttura. Sono i sistemi amministrativi, finanziari e dipartimentali che interagiscono secondo diverse modalità con il fascicolo sanitario, all'interno dei quali si può definire la categoria degli *specialized source system* per individuare i dati provenienti da sorgenti di specialità clinica (quali cardiologia, servizi di emergenza, ecc.).

Occorre, poi, prevedere una serie di sistemi informativi clinici (*clinical information system* (CIS)), i quali si occupano della raccolta e dell'elaborazione dei dati per supportare specifiche funzionalità. Ad esempio, all'interno di un ospedale i sistemi clinici possono essere suddivisi in moduli separati con riferimento a diversi tipi di funzioni.

Abbiamo, inoltre, un'infrastruttura di supporto (*supporting infrastructure*) che riunisce i dati, integrandoli tra di loro. Sebbene ognuno dei sistemi informativi clinici possa tranquillamente funzionare come isola a sé stante di dati, la maggior parte delle strutture sanitarie considera un obiettivo da raggiungere quello dell'integrazione di tutte le informazioni provenienti dai diversi sistemi di approvvigionamento. Un *repository* clinico di dati (*clinical data repository* (CDR)) risponde a tale esigenza: esso consiste in un *database* concepito per gestire i trasferimenti di dati all'interno del sistema. Un «motore di regole» (*rules engine*), ossia un sistema in grado di fungere da fonte di istruzioni operative, fornisce al CDR una logica di programmazione per il supporto alle decisioni cliniche da applicare ai diversi dati all'interno del *repository*. Un *sources knowledge* garantisce, poi, che le informazioni contenute siano rese disponibili e possano così essere utilizzate assieme ai dati raccolti attraverso il EHR (quale, ad esempio, un *database* sui vari tipi di farmaci che descrive i principi attivi e come questi influenzino o possano essere condizionati dai diversi stati fisiologici).

Un'altra struttura di integrazione è rappresentata dal *data warehouse*, in cui i dati specifici possono essere aggregati ed analizzati, al

fine di generare nuove conoscenze. Le componenti volte ad integrare i dati generano a loro volta dei *report*. Infine, i sistemi di archiviazione (*storage system*) sono deputati alla raccolta ed alla conservazione dei dati così ottenuti.

Considerato che la facilità nell'utilizzo di questo tipo di strumenti, unita alla necessaria fiducia che gli utenti devono poter riporre sul sistema stesso, sono i fattori chiave che ne determineranno, o non, il successo, risultano di fondamentale importanza altri due elementi: lo «strato» relativo alla presentazione grafica (*presentation layer*) e l'interfaccia uomo-computer (*human-computer interfaces*). Il primo è quella parte che garantisce l'immissione dei dati e le funzioni di ricerca; questo *software* consente l'utilizzo di *template*, icone ed altre caratteristiche grafiche per la visualizzazione dei dati. La seconda consiste nel dispositivo di *input* con cui gli utenti inseriscono e ricercano i dati (ad esempio, computer *workstation*, *personal* computer, computer portatili, *tablet*, ecc.).

Le funzionalità legate alla connettività del sistema supportano la raccolta e l'integrazione dei dati. Un utilizzo crescente di EHR nel processo curativo dei pazienti, anche in una prospettiva aggregata, richiede una struttura informatica, *hardware* e *software*, che permetta la comunicazione di dati tra reti informatiche locali (*local area network* – LAN[48]) e reti geografiche (*wide area network* – WAN[49]) in modo sicuro e *privacy-oriented*. Il risultato consiste nella creazione di varie forme di scambio di informazioni sanitarie – *health information exchange* (HIE) – tra diverse organizzazioni.

Rimane, in chiusura, da registrare l'importanza che via via stanno acquisendo le fonti di dati che derivano direttamente dai pazienti. Le PHR rappresentano sicuramente il futuro della sanità elettronica

[48] Rete informatica caratterizzata da un'estensione territoriale non superiore a qualche chilometro.

[49] Rete informatica con estensione territoriale pari ad una o più regioni geografiche.

e, dunque, sempre più sarà necessario integrare all'interno dei sistemi già esistenti (EHR) funzionalità ed applicazioni che consentano al paziente-utente di fruire appieno delle potenzialità schiuse dal nuovo ruolo di protagonista della gestione dei percorsi curativi che lo riguardano, a quest'ultimo concesso dalla evoluzione tecnologica.

3.3 Obiettivi di un'infrastruttura di sanità elettronica

Un'infrastruttura di sanità elettronica, quale il EHR (o FSE nella versione italiana), deve avere alcuni obiettivi strategici sui quali puntare. Di seguito elenchiamo i principali requisiti che un sistema informativo volto a gestire i dati sanitari dovrebbe presentare[50].

Innanzitutto, punto fondamentale dev'essere la disponibilità delle informazioni cliniche. La digitalizzazione della documentazione sanitaria deve giungere alla sua completa affermazione, in modo tale che da qualsiasi punto d'accesso del sistema e da parte di qualsiasi utente (paziente, operatore sanitario, ecc.) si possano raggiungere e consultare le informazioni archiviate al suo interno. L'utilità e la forza di un sistema di EHR sono, infatti, costituite dalla possibilità di poter accedere in maniera efficiente, in termini di tempo e di costi, ai dati di un paziente avendo sempre a disposizione l'intera sua storia clinica. Ciò, evidentemente, determina un aumento esponenziale delle capacità di cura di quest'ultimo da parte della struttura sanitaria.

Occorre, poi, puntare su un'architettura federata. Tale assunto rimane un fondamentale obiettivo da raggiungere. Troppo spesso la sanità elettronica si è sviluppata come un'esperienza localistica di alcune realtà virtuose senza che una visione d'insieme, a livello nazionale

[50] Si riprende, commentandola, l'elencazione proposta dal TAVOLO DI LAVORO PERMANENTE SANITÀ ELETTRONICA DELLE REGIONI E DELLE PROVINCE AUTONOME (TSE), *Strategia architetturale per la Sanità Elettronica*, 31 marzo 2006, 14-15, in Rete: <http://www.innovazionepa.gov.it/media/566290/tse-ibse-strategia_architetturale-v01.00-def.pdf>.

quando non internazionale, guidasse e determinasse le scelte più importanti, specialmente in termini di interoperabilità e di standard condivisi. Anche a livello di singola azienda sanitaria sovente si è proceduto ad una stratificazione, talvolta casuale, di infrastrutture informatiche senza aver riguardo alla compatibilità di standard e procedure nemmeno all'interno della stessa realtà di riferimento. È necessario, quindi, cambiare prospettiva ed investire sulla potenzialità propria delle nostre esperienze regionali, costruendo un'architettura tecnico-giuridica che le inserisca come tasselli di un unico mosaico nazionale e federato.

Anche in quest'ambito, come in tutte le architetture digitali, gli aspetti di sicurezza e di privacy giocano un ruolo fondamentale, e ciò implica il perseguimento di ulteriori obiettivi legati all'affidabilità ed alla disponibilità dei dati che l'infrastruttura deve garantire. Essi rappresentano, infatti, concetti chiave per la costruzione di un sistema sicuro e rispettoso dei diritti dei singoli utenti[51].

L'infrastruttura deve essere, poi, ideata in maniera modulare. È un concetto questo che si ritroverà spesso quando si analizzeranno gli aspetti giuridici dei sistemi di FSE alla luce delle indicazioni del Garante Privacy italiano. La modularità è da concepirsi su due livelli. Da un punto di vista interno al sistema, e con particolare riferimento agli utenti, occorre apprestare soluzioni tecniche che permettano l'esercizio del

[51] Cfr. L. DEMUYNCK, B. DE DECKER, *Privacy-Preserving Electronic Health Records*, in J. DITTMANN, S. KATZENBEISSER, A. UHL (a cura di), *Communications and Multimedia Security*. 9th IFIP TC-6 TC-11 Conference, CMS 2005, Salzburg, Austria, September 2005 Proceedings, Laxemburg, Austria, 2005, 150-159, spec. 150 dove si legge: «There are, however, serious privacy concerns associated with the move towards electronic health records. Medical data should not only be protected against outsiders, but also against insiders. Studies have shown that patients do not trust central authorities with their medical data. They want to decide themselves who is entrusted with this data and who is not. (…) Next to patients, healthcare providers want their privacy to be protected. A central repository of medical data controlled by strong access regulations allows for the monitoring of a doctor's actions. Central authorities can track down who is treated by which doctor, how, and for what reasons. Hence, patient-doctor autonomy is disrupted».

diritto di autodeterminazione con riferimento alle informazioni che riguardano un individuo: accesso modulare, oscuramento dei dati, sistemi di catalogazione pensati sulle reali esigenze di cura sono tutte possibili declinazioni del medesimo concetto. Da un punto di vista esterno al sistema, invece, appare necessario concepire le applicazioni di sanità elettronica in modo tale da permettere loro di evolvere indipendentemente le une dalle altre, senza che ciò abbia un impatto sul sistema stesso nel suo complesso. Questo anche e soprattutto per evitarne una rapida obsolescenza.

Infine, l'infrastruttura deve integrarsi con i sistemi già esistenti. È condivisa l'idea che l'implementazione di strutture informatiche di questo tipo non possa avvenire in un'unica soluzione, ma debba anzi procedere per fasi successive al fine sia di permettere agli utenti di cambiare gradatamente i propri stili di vita e il proprio modo di accedere ai servizi sanitari, sia di consentire la risoluzione di problemi che l'utilizzo della struttura stessa sicuramente determinerà, adattandosi alle innumerevoli sfaccettature che la professione medica presenta nella vita reale.

Un'ultima riflessione merita l'utilizzo di standard disponibili pubblicamente (i c.d. *open standard*)[52]. Si tratta di un requisito imprescindibile per un sistema di sanità elettronica che vede nell'interoperabilità la chiave per il successo. Esso non deve riguardare solo i protocolli di trasporto, ma è necessario che anche gli elementi sintattici e semantici comportino l'utilizzo di formati aperti i quali permettano lo scambio e l'utilizzo condiviso di documenti ed informazioni trasmessi tra sistemi.

[52] Per un approfondimento sul tema dell'utilizzo di *open standard* per favorire l'interoperabilità all'interno delle pubbliche amministrazioni, v. L. DE NARDIS, *e-Governance Policies for Interoperability and Open Standards*, Yale Information Society Project Working Paper, June - 2010, in Rete: <http://ssrn.com/abstract=1629833>.

3.4 Intermezzo: sicurezza informatica e computer privacy

Da sempre il diritto si misura con la realtà socio-culturale in cui è chiamato ad intervenire, seguendone gli sviluppi e componendone i conflitti. Per fare questo, il giurista ha bisogno di comprendere a fondo i fenomeni ai quali poi applicherà le regole giuridiche; ha bisogno di assimilare le conoscenze tecniche della scienza alla quale dovrà fornire le regole.

La scienza informatica «parla» inglese: la terminologia, le categorie, la tassonomia della branca scientifica che va sotto il nome di *Computer Security* si esprime in questa lingua. Ogni comparatista sa che il linguaggio è intimamente legato al contesto nel quale si è sviluppato, alla cultura del popolo che lo ha creato. Il comparatista sa anche che il linguaggio tecnico, sia esso giuridico o informatico, si caratterizza per la complessità dei significati associati alle parole che rendono il lavoro di traduzione e di comparazione particolarmente laborioso[53]. L'informatica conosce un linguaggio di «koiné». Il giurista si trova di fronte ad un nuovo problema: comparare esperienze, ordinamenti giuridici diversi in riferimento alle regole adottate per disciplinare il fenomeno della digitalizzazione e comparare poi questi con un linguaggio tecnico che si esprime in inglese ma che è frutto di una comunità (scientifica) diversa da quella giuridica (e il cui oggetto di studio non

[53] «"When I used a word", Humpty Dumpty said, in a rather scornful tone, "it means just what I choose it to mean-neither more nor less". "The question is", said Alice, "whether you can make words mean so many different things". "The question is", said Humpty Dumpty, "which is to be master-that's all"», in *Alice in Wonderworld*. Per approfondimenti, in prima approssimazione, v. S. CAVAGNOLI, E. IORIATTI FERRARI, *Tradurre il diritto. Nozioni di diritto e di linguistica giuridica*, Padova, 2009; E. IORIATTI FERRARI (a cura di), *La traduzione del diritto comunitario ed europeo: riflessioni metodologiche*. Atti del Convegno tenuto presso la Facoltà di Giurisprudenza di Trento 10-11 marzo 2006, Trento, 2007; A. GAMBARO, *Comprendere le strategie comunicative del legislatore*, in *Riv. crit. dir. priv*., 2000, 605, R. SACCO, *Traduzione giuridica* [aggiornamento-2000], in *Digesto civ*., Torino, 722.

risulta essere frammentato dai confini nazionali). Occorre chiarire quale significato associamo ai termini ed alle categorie che usiamo e sgombrare il campo da definizioni fuorvianti.

È opportuno, pertanto, includere nella trattazione tecnica svolta in questo capitolo alcune considerazioni legate all'importanza che rivestono in tale contesto concetti di confine tra la scienza giuridica e quella informatica: quelli della sicurezza e della privacy informatica[54].

Lo sviluppo delle tecnologie digitali e la diffusione nella società dei computer ha reso sempre più evidente la necessità di programmare ed implementare strumenti via via più evoluti, volti a proteggere i file e le informazioni raccolte nelle banche dati (si parla appunto di *Computer Security*). La Rete ha poi colorato di nuove sfumature questo settore di studio. L'affermarsi di sistemi c.d. *distributed* ed il diffondersi di reti di comunicazione tra i diversi terminali, infatti, ha sollevato un nuovo problema: la tutela dell'integrità dei dati durante la loro trasmissione. Il termine *network security* individua, appunto, questa sottocategoria della sicurezza informatica, la quale focalizza la propria attenzione sugli strumenti che consentono le comunicazioni intercorrenti tra i vari punti e nodi di una rete. Posto che Internet è definita come la rete delle reti, si parla anche di *Internet security*[55].

---

[54] Cfr. CACCIA, *Management dei sistemi informativi in sanità*, cit., 4-190; GARTEE, *Electronic Health Records*, cit., 371-409; CARTER, *Electronic Health Records*, cit., 295-324; TAVOLO DI LAVORO PERMANENTE SANITÀ ELETTRONICA DELLE REGIONI E DELLE PROVINCE AUTONOME (TSE), *Strategia architetturale per la Sanità Elettronica*, cit., 30-33.

[55] Il tema delle architetture informatiche è oggetto di analisi anche nella psicologia, in quanto dipende da un modo di sentire che non si basa sulla probabilità e sui calcoli matematici ma sulle reazioni psicologiche che abbiamo di fronte ai rischi ed alle misure di protezione. Da qui l'acquisita consapevolezza che la protezione dei dati personali rappresenti una sorta di *trade-off*, di bilanciamento nelle scelte tra i guadagni rispetto ad un certo obiettivo e le contemporanee perdite riguardo ad un altro. Vedi gli ottimi approfondimenti di quello che viene considerato un «guru» della *computer security*, Bruce Schneier, reperibili sul suo *blog* «Schneier on Security»: <http://www.schneier.com/blog/>. Tra gli altri si segnalano: B. SCHNEIER, *The Psychology of Security*, 2008,

La scienza informatica nel campo della *computer security* si basa su alcuni principi che, sulla scorta dei principi giuridici, caratterizzano e condizionano l'analisi dei diversi contesti in cui essa poi si estrinseca. La loro definizione è oggetto di dibattiti ed approfondimenti da parte della dottrina scientifica. Di seguito si cercherà di enuclearli, con l'intento di fornire le classificazioni indispensabili per un approccio interdisciplinare alla materia della sicurezza informatica, declinata sul piano della protezione dei dati personali[56].

Il primo aspetto che prendiamo in esame è quello della c.d. *confidentiality* (riservatezza)[57], ovvero il tentativo di prevenire la divulgazione non autorizzata delle informazioni. In passato, sicurezza e segretezza erano concetti intimamente correlati. L'obiettivo principale della sicurezza è anzi quello di impedire agli utenti non autorizzati l'accesso alle informazioni riservate. La *confidentiality*, intesa nei due aspetti che la caratterizzano, privacy e *secrecy*, coglie questo aspetto della *computer security*. Il termine privacy è, però, distinto da quello di *secrecy*: il primo si riferisce principalmente alla protezione dei dati personali; il secondo riguarda invece la protezione dei dati posseduti da un'organizzazione. La riservatezza rappresenta certamente un punto di riferimento nell'ambito della sicurezza dei dati personali, stante il fatto che, con

---

in Rete: <http://www.schneier.com/essay-155.html>; ID., *Beyond Fear. Thinking Sensibly about Security in an Uncertain World*, New York, 2003. L'autore individua cinque aspetti specifici del *trade-off* di sicurezza su cui un individuo può essere portato a sbagliare: a) il grado di rischio, b) la probabilità del rischio, c) il valore dei costi, d) l'efficacia della misura di protezione nel mitigare il rischio, e) il *trade-off* stesso.

[56] Per approfondimenti sul tema della sicurezza informatica v. R. ANDERSON, *Security Engineering. A Guide to Building Dependable Distributed Systems*, Wiley, 2001, 3 ss. in Rete: <http://www.cl.cam.ac.uk/%7Erja14/book.html>; D. GOLLMAN, *Computer Security*, II ed., Chichester, 2006, 17 ss.; W. STALLINGS, *Network Security Essentials: Applications and Standards*, III ed., Upper Saddle River, New Jersey, 2007, 11 ss.

[57] Proporremo sempre una traduzione italiana del termine informatico in inglese: essa dovrà essere presa *cum grano salis* stante la difficoltà di tale operazione alla luce anche delle considerazioni svolte sopra sui problemi legati alla traducibilità dei termini tecnici.

l'implementazione di tale principio attraverso una serie di applicazioni e strumenti informatici, si cerca di impedire da parte di soggetti non autorizzati l'accesso alle informazioni contenute all'interno del sistema oggetto di trasmissione, garantendo così la riservatezza delle informazioni stesse.

Per quanto riguarda il concetto di *integrity* (integrità) troviamo una definizione precisa nell'*Orange Book* (*US Department of Defense*, 1985) che la intende come

> the state that exists when computerized data is the same as that in the source documents and has not been exposed to accidental or malicious alteration or destruction.

L'accento viene posto sulla necessità che i dati immagazzinati all'interno di un sistema informatico corrispondano a qualcosa di reale ed esterno al sistema stesso, richiamando, in questo modo, un altro concetto strettamente ed inscindibilmente collegato a quello di integrità, l'*authenticity* (autenticità). Ad un livello di ancora maggiore dettaglio, nell'ambito della sicurezza delle comunicazioni, essa riguarda la rilevazione di correzioni, modificazioni, cancellazioni o ripetizioni dei dati trasmessi. Inoltre, l'*integrity* è spesso un prerequisito per altre qualità della sicurezza, in quanto, ad esempio, essa garantisce la possibilità di rilevare e reagire a possibili modificazioni del sistema informatico volte a compromettere la confidenzialità dei dati in esso contenuti. Sul versante della protezione dei dati personali, questo principio fa da *pendant* con il diritto riconosciuto al soggetto titolare dei dati a vedere quest'ultimi aggiornati, corretti, modificati o cancellati.

L'*availability* (disponibilità) indica, invece,

> the property of being accessible and useable upon demand by an authorized entity[58].

Essa si pone oltre i tradizionali confini della sicurezza informatica e riguarda problemi che si profilano ad un livello più generale. Si vuole garantire che un attacco intenzionale proveniente dall'esterno non possa alterare le funzionalità del sistema impedendo agli utenti autorizzati di accedere alle risorse del sistema stesso. In molte situazioni, l'*availability* può rappresentare uno degli aspetti più importanti per garantire la sicurezza di un sistema.

Alla luce dei problemi sopra evidenziati occorre essere consapevoli di un aspetto centrale nella sicurezza, ossia del fatto che difficilmente si sarà in grado di predisporre un sistema idoneo a prevenire qualsivoglia attività impropria. Azioni senza dubbio autorizzate potrebbero comunque determinare una violazione della sicurezza. Inoltre, possono esservi difetti che permettono al soggetto che intende porre in essere un'attività non permessa di aggirare il controllo. Il sistema deve, allora, poter individuare e determinare le responsabilità degli utenti. L'*accountability* (responsabilità, o più precisamente la capacità di rintracciare coloro che abbiano infranto una *policy*) richiede che

> audit information must be selectively kept and protected so that actions affecting security can be traced to the responsible party[59].

Per fare ciò il sistema dev'essere in grado di identificare ed autenticare gli utilizzatori e deve tenere un aggiornato registro in grado di tracciare in maniera accurata (*audit trail*) gli eventi rilevanti per il fine della sicurezza.

---

[58] Definizione rinvenibile nell'ISO 7498-2 (*International Organization for Standardization*, 1989).

[59] Ancora una definizione tratta dall'*Orange Book*.

La *nonrepudiation* assicura che un rapporto di «delegazione» non possa essere poi disconosciuto da alcuna delle parti coinvolte[60]. Nel contesto giuridico essa risponde a due esigenze: quella di garantire la certezza nel momento della conclusione di un accordo e quella di costituire un sistema di prove che permettano di determinare *ex post* il contenuto dell'accordo stesso. La *nonrepudiation* è una categoria utilizzata in quegli studi che si prefiggono di trovare soluzioni atte a prevenire i conflitti di interesse nelle *delegation chain*, ovvero in quelle catene di delega di permessi (*delegation of permission*) e di operazioni da porre in essere (*delegation of execution*) che gli informatici ben conoscono[61]. I *nonrepudiation service* forniscono la prova (la più certa possibile) che una determinata azione si è verificata. Quando si vuole garantire la *nonrepudiation* spesso ci si riferisce alla firma digitale, che si basa sulla crittografia e si sostanzia nell'utilizzo di chiavi asimmetriche[62].

Infine, altra nozione fondamentale nella sicurezza informatica è quella di *dependability* (affidabilità), la quale può essere definita come la capacità di un sistema informatico di fornire un servizio che può essere considerato «fidato»[63]. La *dependability* è, in realtà, un concetto

[60] Non si formula la traduzione in italiano di questo termine perché risulta impossibile renderne il significato senza utilizzare una perifrasi.

[61] Sul problema dei *conflict of interest* in ambito informatico, v., *ex plurimis*, F. MASSACCI, N. ZANNONE, *Detecting Conflicts between Functional and Security Requirements with Secure Tropos: John Rusnak and the Allied Irish Bank*, Technical Report DIT-06-002, University of Trento, 2006.

[62] Ai sensi dell'art. 1, co. 1, lett. s, d.lgs. 7 marzo 2005, n. 82 («Codice dell'amministrazione digitale»; d'ora in avanti CAD) la «firma digitale» consiste in «un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici».

[63] Il IFIP WG 10.4 (*International Federation for Internet Processing Working Group* 10.4, fondato nel 1980) fornisce una definizione di *dependability*: «[..] the trustworthiness of a computing system which allows reliance to be justifiably placed on the

che include diversi attributi, per alcuni dei quali abbiamo già fornito sopra una descrizione: *availability*; sicurezza, intesa come compresenza di *confidentiality* ed *integrity*; *reliability* (affidabilità), cioè la capacità del sistema di rispettare le specifiche di funzionamento nel tempo; *safety*, ovvero l'assenza di eventi lesivi a danno degli utenti (eventi che dipendono dall'ambiente circostante).

Nel contesto sanitario, infine, acquista notevole importanza anche l'aspetto della modularizzazione nell'accesso ai dati, espressione tecnica del principio di autodeterminazione che deve caratterizzare l'utilizzo da parte del paziente-utente del sistema delle infrastrutture di FSE (o EHR che dir si voglia).

Sicurezza e protezione dei dati, pertanto, si intersecano: solo un sistema in grado di garantire il rispetto della seconda riesce a fornire uno strumento sicuro agli operatori ed ai fruitori in generale del nuovo servizio informatico.

Esistono, infine, diversi approcci alla sicurezza informatica[64]. Tra le numerose proposte per affrontare il problema troviamo delle soluzioni più prettamente «ingegneristiche»: queste propongono di ridisegnare i sistemi operativi al fine di renderli più sicuri; altre opzioni suggeriscono, invece, di modificare le metodologie di programmazione. Altri approcci ancora si concentrano sulla necessità di modificare l'*hardware* stesso dei *personal* computer. L'ultimo approdo è qui rappresentato dal c.d. *Trusted Computing* (TC), tecnologia innovativa derivata dai lavori svolti dal *Trusted Computing Group* (TCG)[65]. Tale

---

service it delivers [..]». V. anche A. AVIZIENIS, J.C. LATRIE, B. RANDELL, *Fundamental Concepts of Dependability*, Research Report N01145, LAAS-CNRS, 2001.

[64] Sull'argomento v. in generale S. SCHOEN, *Trusted Computing: Promise and Risk*, in Rete: <http://www.eff.org/Infrastructure/trusted_computing/20031001_tc.php>.

[65] Il nucleo iniziale del *Trusted Computing* risiedeva nella *Trusted Computing Platform Alliance* (TCPA) fondata da Compaq, HP, IBM, Intel e Microsoft. I compiti di quest'ultima sono stati, poi, assorbiti ed ampliati dal *Trusted Computing Group* (TCG), un'organizzazione no-profit promossa da sette imprese (le cinque fondatrici della TCPA oltre a Sony Corporation e Sun Microsystems, Inc.). V. il sito web:

progetto è teso a sviluppare, definire e promuovere specifiche per ottenere standard aperti di *hardware*: l'obiettivo è quello di creare ambienti informatici più sicuri di quelli attuali senza per questo compromettere l'integrità funzionale di siffatti sistemi, della privacy e dei diritti individuali. Tutto questo dovrebbe realizzarsi promuovendo la costruzione di sistemi *hardware* e *software* non abilitati a determinate funzioni, che siano in potenza in grado di comprometterne la sicurezza, nonché di promuovere il controllo – attraverso Internet – del rispetto delle limitazioni di funzionalità da parte degli utenti dei sistemi[66]. La logica TC si basa sull'assunto che la sicurezza di un computer possa essere messa a rischio dal proprietario o dall'utente del computer stesso. Il tutto si estrinseca in due fondamenti: il primo è dato dalla limitazione preventiva (e fisica) delle funzionalità del sistema informatico; il secondo risiede nella dislocazione del controllo del sistema informatico dall'utente finale verso i soggetti che producono l'*hardware* ed il *software*, nonché verso quelli che sono deputati a sorvegliare – mediante Internet – il rispetto delle limitazioni di funzionalità imposte dal produttore[67].

<http://www.trustedcomputinggroup.org>. Per approfondimenti, v. R. CASO, *Un "rapporto di minoranza": elogio dell'insicurezza informatica e della fallibilità del diritto. Note a margine del Trusted Computing*, in R. CASO (a cura di), *Sicurezza informatica: regole e prassi*. Atti del Convegno tenuto presso la Facoltà di Giurisprudenza di Trento il 6 maggio 2005, Trento, 2006, 4 ss.

[66] Il computer rappresenta sempre più una proiezione della nostra esistenza, delle nostre faccende quotidiane, delle nostre emozioni. Questo tipo di approccio pone due problemi di fondo, estremamente rilevanti su un piano giuridico. Innanzitutto, il processo di elaborazione degli standard tecnologici dell'architettura TC, così come la sicurezza di essa, è riposto completamente nelle mani di privati, i quali non necessariamente agiscono in base a processi trasparenti e democratici. Inoltre, la sicurezza dipende dall'architettura informatica la quale incorpora alcune regole implicite, che si connotano per rigidità, predeterminatezza e potenziale infallibilità; diversamente dal diritto che, invece, è per sua natura caratterizzato da regole elastiche, verificabili solo *ex post* e sempre potenzialmente fallibili. Sul punto v. CASO, *Un "rapporto di minoranza"*, cit., *passim*.

[67] Lo scopo principale consisterebbe, a detta dei fautori di questa proposta, nell'aiutare gli utenti a proteggere il proprio patrimonio di informazioni sia dagli attac-

L'approccio ora descritto è stato, come prevedibile, oggetto di numerose ed accese critiche[68].

4. L'importanza degli standard

4.1 Premesse metodologiche

La storia della tecnica può essere descritta come la storia del tentativo dell'uomo di asservire le leggi della natura ai propri bisogni e di rompere, in un certo qual modo, la «temporalità ciclica» che la caratterizza, resistendo così ai suoi effetti sulle orme del titano Prometeo che rubò il fuoco agli dei per donarlo agli uomini[69].

Fin dalle origini della storia dell'umanità l'uomo ha sviluppato nuove tecnologie; anzi, possiamo dire che tale capacità lo distingue da tutti gli altri esseri viventi. Con il trascorrere del tempo, però, i mezzi tecnici sono aumentati a tal punto, in numero e potenza, che l'uomo ha finito per perdere il completo controllo e dominio su di essi, provocando un significativo rovesciamento dei ruoli[70]. Se in precedenza, infatti,

---

chi compiuti mediante *software* sia dagli attacchi fisici. V. il sito web: <https://www.trustedcomputinggroup.org/about/>. Teniamo sempre presente il fatto che generalmente in ambito informatico ciò che aumenta il livello di sicurezza tende a diminuire quello di protezione della privacy.

[68] V., fra tutte, le osservazioni sollevate da R. ANDERSON, *'Trusted Computing' Frequently Asked Question*, Versione 1.1 agosto 2003, in Rete: <http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html>.

[69] Cfr. U. GALIMBERTI, *Psiche e techne. L'uomo nell'era della tecnica*, Milano, 1999, 78. Per un approfondimento in chiave giuridica, v. F. SALMONI, *Le norme tecniche*, Milano, 2001. Cfr. anche D. FISICHELLA, *L'altro potere - Tecnocrazia e gruppi di pressione*, Roma - Bari, 1997. V. un'interessante riflessione sul rapporto tra uomo e tecnica alla luce del mito di Prometeo in R. TRABUCCHI, *Prometeo e la sopravvivenza dell'uomo – Tecnica e prassi per il terzo millennio*, Milano, 1998.

[70] Cfr. D. GRIMM, *Il futuro della Costituzione*, in G. ZAGREBELSKY, P.P. PORTINAIO, J. LUTHER (a cura di), *Il futuro della Costituzione*, Torino, 1996, 129 ss. V. anche E. SEVERINO, *Il destino della tecnica*, Milano, 1998.

la tecnica rappresentava uno strumento in grado di far raggiungere all'uomo gli obiettivi verso i quali tendeva la propria azione, ora essa aumenta quantitativamente e qualitativamente la realizzazione di qualsiasi fine concepibile. Non è così

> […] più il fine a condizionare la rappresentazione, la ricerca, l'acquisizione dei mezzi tecnici, ma sarà la cresciuta disponibilità dei mezzi tecnici a dispiegare il ventaglio di qualsivoglia fine che per loro tramite può essere raggiunto[71].

La tecnica cerca di dissimulare l'incremento della propria potenza, tentando di accreditare la propria sostanziale diversità rispetto al potere politico per il suo essere neutrale ed oggettiva, in quanto mera applicazione delle leggi della scienza e della natura[72]. Tuttavia la tecnica è, già alla sua nascita, volontà di potenza: volontà dell'uomo di sosti-

[71] Cfr. GALIMBERTI, *Psiche e techne*, cit., 37.

[72] Cfr. M. MANETTI, *Poteri neutrali e Costituzione*, Milano, 1994, 95 ss. Con particolare riferimento alle architetture informatiche Lessig approfondisce il tema della non neutralità della tecnologia ai valori (*not-value neutral*): v. L. LESSIG, *Code v. 2*.0, New York, 2006, (in Rete: <http://codev2.cc/>) in part. 125 dove si legge: «They [code writers] constrain some behavior by making other behavior possible or impossible. The code embeds certain values or makes certain values impossible. In this sense, it too is regulation, just as the architectures of real-space codes are regulations»; considerazioni analoghe sono svolte in un'altra sua opera ID., *Code and other Laws of Cyberspace*, New York, 1999, dove l'autore sottolinea che non è la regola giuridica che prevale quale strumento regolativo nel contesto digitale, bensì i comandi incorporati all'interno dei protocolli di comunicazione di Internet e le applicazioni *software*. Un'opinione parzialmente difforme in E. DOMMERING, *Regulating technology: code is not law*, in E. DOMMERING, L. ASSCHER (a cura di), *Coding Regulation. Essays on the Normative Role of Information Technology*, The Hague, 2006, 1-16, in part. 1, ove si legge: «much of the cyberspace argument can be retraced to the general problem of regulating technology, that is to say: regulating the side-effects of technology on human society by means of law-based rules and by technical means» e «my argument is that any technology, not only by its 'architecture' but also by the social function society attributes to technical innovations, *eo ipso* is a normative concept». Sulla questione v. anche L. ASSCHER, *'Code' as Law. Using Fuller to Assess Code Rules*, *id.*, 61-90.

tuirsi al divino (riprendiamo qui il mito di Prometeo) per sconfiggere la natura. In quanto volontà di potenza essa non è, quindi, pensabile come qualcosa di neutrale, di oggettivo, di spoliticizzato[73].

Occorre, quindi, cercare di coniugare la tecnica al diritto (ed alla morale), restituendo quest'ultimo alla dignità che gli compete e rivendicandone la superiorità[74].

Lo sviluppo scientifico e tecnologico non ha solamente pervaso la vita sociale e politica degli individui, ma ha inevitabilmente influenzato anche il diritto, condizionando in maniera determinante l'azione dei poteri pubblici.

Le implicazioni e relazioni reciproche tra tecnica e diritto sono oramai cosa certa ed incontestabile. Anzi, con lo svilupparsi delle tecnologie digitali tali legami tendono a crescere esponenzialmente. Il diritto ha sempre più bisogno della tecnica, senza la quale non sarebbe in grado di disciplinare un gran numero di rapporti, che, solo grazie alla conoscenza di essa e delle sue prescrizioni, possono venire regolamentati (si pensi all'ambito delle comunicazioni e della nascente e controversa disciplina delle biobanche, ecc.)[75].

---

[73] La tecnica, infatti, «può essere rivoluzionaria e reazionaria, può servire alla libertà e all'oppressione, alla centralizzazione e alla decentralizzazione», in C. SCHMITT, *L'epoca delle neutralizzazioni e delle politicizzazioni*, in G. MIGLIO, P. SCHIERA (a cura di), *Le categorie del politico*, Bologna, 1972, 179. L'autore si spinge oltre ed afferma che la tecnica è «culturalmente cieca». Per approfondimenti v. J. ELLUL, *Il sistema tecnico. La gabbia delle società contemporanee*, Milano, 2009 (trad. it. di G. CARBONELLI; titolo originale: *Le Système technicien*, 1977), in part. 1, ove si legge: «La tecnica non si accontenta di *essere*, e, nel nostro mondo, di essere *il fattore principale* o determinante: essa è divenuta Sistema».

[74] Cfr. N. IRTI, E. SEVERINO, *Le domande del giurista e le risposte del filosofo (un dialogo su diritto e tecnica)*, in *Contr. e impr.*, 2000, 665; L. MENGONI, *Diritto e tecnica*, in *Riv. trim. dir. e proc.*, 2001, 1.

[75] Cfr. U. FADINI, *Norma e mondo nell'era della tecnica*, in *Dem. dir.*, 1987, 25; S. RODOTÀ, *Tecnologie e diritti*, Bologna, 1995; L. D'AVACK, *Ordine giuridico e ordine tecnologico*, Torino, 1998.

Dalla metà del Novecento, alcuni studiosi si sono concentrati sul momento della produzione delle norme tecniche, rivolgendo la loro attenzione all'attività dei c.d. esperti: la produzione delle norme e regole tecniche comincia a venire «svelata» e vengono messi in luce gli attuali e concreti pericoli per la democrazia[76]. Il fatto che la produzione normativa tecnica venga completamente affidata a soggetti dotati di elevate conoscenze specialistiche e, in quanto tali, più idonei a disciplinare le materie tecniche, almeno più di quanto non lo siano gli organi deputati naturalmente alla produzione di norme giuridiche, ha indotto la dottrina a concentrare la propria attenzione sul grave problema della graduale erosione della sovranità statale da parte di soggetti pubblici e privati spesso di carattere sovra-nazionale[77].

Gli organi cui tradizionalmente lo Stato ha distribuito e delegato i propri poteri vengono sempre più delegittimati e privati delle loro prerogative. Si assiste al tentativo di sostituire lo Stato sovrano con qualche cosa di diverso, che alcuni studiosi, enfaticamente, hanno definito «l'antisovrano»: questo

> […] non è un soggetto (ma semmai una pluralità di soggetti…); non dichiara la propria aspirazione all'assoluta discrezionalità del proprio potere (cerca anzi di presentare le proprie decisioni come logiche deduzioni di leggi generali oggettive…); non reclama una legittimazione trascendente […] ma immanente […]; non pretende di ordinare un gruppo sociale dotato di almeno un minimum d'omogeneità (il popolo

[76] Cfr. P. BIONDINI, *Approcci definitori alla "norma tecnica"*, in N. GRECO (a cura di), *Crisi del diritto, tecnica in campo ambientale*, Roma, 1999, 31; M. GIGANTE, *Alcune osservazioni sull'evoluzione dell'uso del concetto di tecnica*, in *Giur. cost*., 1997, 647; SALMONI, *Le norme tecniche*, cit., 31 ss.

[77] Cfr. L. FERRAJOLI, *La sovranità nel mondo moderno. Nascita e crisi dello Stato nazionale*, Roma – Bari, 1997; G. SILVESTRI, *La parabola della sovranità. Ascesa declino e trasfigurazione di un concetto*, in *Riv. dir. cost*., 1996, 3; A. PRADIERI, *Le norme tecniche nello Stato pluralista e prefederativo*, in *Il diritto dell'economia*, 1996, 251; M. LUCIANI, *L'antisovrano e la crisi delle Costituzioni*, in *Riv. dir. cost*., 1996, 731; SALMONI, *Le norme tecniche*, cit., 228 ss.

> di una nazione), ma una pluralità indistinta, anzi la totalità dei gruppi sociali (tutti i popoli di tutto il mondo, o almeno tutti i popoli della parte del mondo che si ritiene meritevole di interesse); non vuol essere l'espressione di una volontà di eguali formata dal basso[78].

La globalizzazione dell'economia elimina i confini nazionali, omogeneizza le culture e di conseguenza riduce le differenze; così facendo, però, finisce anche con l'erodere la sovranità degli Stati[79]. Nell'era, quindi, del sovrano transnazionale e tecnologico, i tradizionali poteri dello Stato hanno la necessità di trovare una loro collocazione nel sistema. Tornano così in voga concetti e riflessioni che si pensavano abbandonati, quale ad esempio quello della certezza del diritto, intesa come una volontà eguale e costante della legge, che deve, però, fare i conti con le esigenze di cambiamento, alimentate dalla tecnica e dello sviluppo economico[80]. È, dunque, profondamente avvertita la necessità di conciliare il mondo del diritto con quello della tecnica e di ricondurre, così, l'efficacia di quest'ultima nell'ambito della legittimità.

4.2 Gli standard nella sanità elettronica

Nel contesto delle ICT è di cruciale importanza che le informazioni possano essere condivise all'interno delle varie strutture e che le diverse applicazioni e sistemi informatici possano trovare un efficiente livello di integrazione. Al fine di rendere possibile lo scambio e la riutilizzazione di informazioni tra sistemi ed aziende diverse occorre implementare l'uso di standard e di architetture aperti basati sull'interoperabilità. Ciò al fine di poter disporre di informazioni in tempo reale

[78] LUCIANI, *L'antisovrano e la crisi delle Costituzioni*, cit., 780-781.

[79] Si v. le interessanti riflessioni sui caratteri distintivi del diritto dell'era digitale, tra cui, appunto, la destatualizzazione in PASCUZZI, *Il diritto dell'era digitale*, cit., 267 ss., in particolare 291-296.

[80] Cfr. GIGANTE, *Effetti giuridici nel rapporto tra tecnica e diritto: il caso delle norme «armonizzate»*, cit., 317.

ed in modalità telematica, migliorando così la gestione delle risorse aziendali e tenendo sotto costante controllo i risultati conseguiti dall'azienda stessa[81].

Altri concetti di riferimento sono poi l'interconnessione e l'interoperabilità. Col primo si intende la possibilità tecnica di trasferire dati da un sistema ad un altro; col secondo, invece, ci si riferisce alla capacità di comunicare e riutilizzare dati prodotti ed archiviati in un dato sistema verso un altro sistema all'interno di una singola azienda o tra questa ed altre aziende esterne. Se la prima operazione non presenta difficoltà insormontabili, la seconda obbliga alla definizione di accordi relativi alla struttura dei dati scambiati su tre diverse variabili: la semantica, cioè il significato di ciascun campo; la sintassi, ovvero il formato di ciascun campo e la sua rappresentazione; l'ordine col quale i dati elementari sono trasmessi ed il modo in cui debbono essere marcati e resi riconoscibili; il carattere utilizzato per separare i campi[82].

Si è già fatto cenno sopra ai temi legati alle problematicità dei processi che determinano l'emersione degli standard in rapporto alle tradizionali norme giuridiche. Trattando di sanità elettronica citiamo i soggetti istituzionali che, nello specifico, si occupano della standardizzazione in ambio medico-sanitario.

A livello nazionale si ritrova l'UNI-Commissione Informatica Medica. All'interno di essa, recentemente, è stato costituito anche un

[81] Per approfondimenti sugli standard in generale e nello specifico ambito della sanità elettronica v. CARTER, *Electronic Health Records*, cit., 119-141; BUCCOLIERO, CACCIA, NASI, *e-he@lth*, cit., 133-159; GARTEE, *Electronic Health Records*, cit., 39-74; AMATAYAKUL, *Electronic Health Records*, cit., 204 ss.

[82] BUCCOLIERO, CACCIA, NASI, *e-he@lth*, cit., 135-136. Tra i vari modelli di scambio di dati utilizzati, il più semplice è rappresentato dal modello ASCII (solo testo) su supporto fisico (banda magnetica, *floppy disk*, *pen drive*). Altra modalità conosciuta è quella che vede l'uso di c.d. «postini elettronici»: ciò presenta, però, l'inconveniente che, avvenendo la trasmissione di informazioni senza alcun struttura formale, si deve prevedere delle operazioni per la ricomposizione delle informazioni in formati leggibili dagli applicativi. Le *Application Program Interface* (API) rappresentano, infine, un'ulteriore modalità di scambio di dati maggiormente elaborata.

gruppo di lavoro chiamato *Technical Group* su HL7, il quale è impegnato anche nel campo della standardizzazione.

A livello comunitario, invece, opera il CEN TC 251 *Health Informatics*, il quale risulta a sua volta suddiviso in quattro *Working Group*: WG1 *Information Models*, WG2 *Terminology and knowledge bases*, WG3 *Security, Safety and quality*, WG4 *Technology for interoperability*.

A livello internazionale lavora, infine, l'ISO TC 21 *Health Informatics*, il quale, a sua volta, è composto da sei *Working Group*: WG1 *Health records and modelling coordination*, WG2 *Messaging and communication*, WG3 *Health concept representation*, WG4 *Security*, WG5 *Health Cards*, WG6 *e-Pharmacy and medicines business*.

Nell'ambito dell'applicazione delle ICT all'interno del contesto sanitario gli standard utilizzati a livello internazionale sono, principalmente, lo standard DICOM, approvato dall'*International Organization for Standardization* (comunemente conosciuta come ISO)[83] e lo standard HL7, per il quale la certificazione da parte dell'ISO è in fase di approvazione ma che risulta già ampiamente utilizzato come standard *de facto* (esso è stato certificato dall'*American National Standard Institute* (ANSI)[84]). Dell'HL7 sono già state prodotte alcune versioni nazionali. Prima di passare alla descrizione di questi due standard, occorre quantomeno dar conto di altre due iniziative a livello internazionale che lavorano per diffondere l'utilizzo di standard in sanità.

Da un lato, si fa riferimento al progetto internazionale *Integrating the Healthcare Enterprise* (IHE), gruppo di lavoro che opera in sinergia con le associazioni legate alla sanità allo scopo di incrementare l'integrazione in ambito sanitario[85]. Esso non è un ente certificatore,

[83] V. sito web: <http://www.iso.org/iso/home.htm>.

[84] V. sito web: <http://www.ansi.org/>.

[85] V. il sito web: <http://www.ihe.net/>; e la versione europea <http://www.ihe-europe.net/>. Per approfondimenti v. la voce *Integrate the Health Care* su wikipedia: <http://it.wikipedia.org/wiki/Integrate_the_Healtcare_Enterprise>.

bensì è meglio enucleabile come un *forum* sponsorizzato da associazioni di utilizzatori e fornitori al fine di favorire la discussione circa l'implementazione di standard all'interno dei loro prodotti.

Dall'altro, la *Promotion Strategy for European Electronic Healthcare Record* (PROREC), ovvero l'azione europea per la promozione dell'utilizzo di soluzioni finalizzate alla la realizzazione di sistemi EHR. Essa è sostenuta dalla Commissione europea. L'obiettivo principale di PROREC è quello di promuovere e coordinare la convergenza su scala europea verso sistemi di EHR a vocazione generale, sicuri e tra loro interoperabili.

4.2.1 Digital Imaging Communication in Medicine (DICOM)

Digital Imaging and Communications in Medicine (DICOM) è uno standard per la gestione, l'archiviazione, la stampa e la trasmissione di informazioni e di immagini mediche[86]. Comprende una definizione del formato di file e un protocollo di comunicazione di rete. Quest'ultimo consiste in un protocollo applicativo che utilizza il TCP/IP per la comunicazione tra sistemi. Il *National Electrical Manufacturers Association* (NEMA) ha la titolarità del diritto d'autore su questo standard. Esso è stato sviluppato dal DICOM *Standards Committee*, i cui membri sono in parte anche membri del NEMA.

DICOM consente l'integrazione di *scanner*, *server*, *workstation*, stampanti e *hardware* di rete da parte dei produttori in un unico sistema di archiviazione e di comunicazione di immagini (*Picture Archiving and Communication System* (PACS)). I diversi dispositivi sono dotati di dichiarazioni di conformità DICOM, che indicano chiaramente le classi DICOM supportate. DICOM è stato ampiamente adottato dagli

[86] Per approfondimenti v. BUCCOLIERO, CACCIA, NASI, *e-he@lth*, cit., 143-145. V. il sito web: <http://medical.nema.org/>.

ospedali e si sta diffondendo anche in contesti più piccoli, quali studi dentistici ed ambulatori medici.

DICOM è conosciuto come NEMA Standard PS3, e come standard ISO 12.052, ed ha raggiunto un livello quasi universale di utilizzo da parte dei fornitori di apparecchiature di *imaging* medico e delle organizzazioni sanitarie.

4.2.2 Health Level Seven

Health Level Seven (HL7) è un'organizzazione *non-profit* per lo sviluppo di standard di scambio ed integrazione di dati clinici per la gestione dei processi di cura[87]. È stata fondata nel 1987 ed è ufficialmente accreditata in qualità di *Standards Development Organization* presso *l'American National Standards Institute* (ANSI).

Tale organizzazione produce standard di messaggistica per lo scambio di informazioni tra diversi sistemi informativi all'interno di una singola impresa o tra imprese diverse. La partecipazione all'HL7 è su base completamente volontaria. I partecipanti sono organizzati in comitati tecnici ed in speciali gruppi di lavoro. Si tratta di un processo di produzione basato sul consenso. Ogni proposta viene discussa tra i membri del comitato tecnico o del gruppo di lavoro e gli eventuali commenti negativi devono essere risolti prima che essa venga messa ai voti per divenire uno standard HL7.

HL7 si concentra principalmente sullo sviluppo di standard nei settori clinico ed amministrativo. Non presuppone alcuna architettura specifica del sistema informativo e prevede fondamentalmente tre grandi tipi di interazioni fra nodi di comunicazione: l'aggiornamento

[87] Per approfondimenti v. BUCCOLIERO, CACCIA, NASI, *e-he@lth*, cit., 145-158; CARTER, *Electronic Health Records*, cit., 130-133; AMATAYAKUL, *Electronic Health Records*, cit., 269. V. il sito web dell'organizzazione: <http://www.hl7.org/>.

dei dati non sollecitato (*acknoledgment*), l'interrogazione (*query*) e l'invio dei messaggi (notificato in modalità *broadcast*).

HL7 è, ad oggi, uno standard *de facto*[88].

5. Implementazione del Fascicolo Sanitario Elettronico: esperienze nazionali ed estere

5.1 Premessa

Al termine di questo capitolo, dopo aver descritto nelle sue linee fondamentali il contesto all'interno del quale le esperienze di sanità elettronica sono maturate ed aver riservato spazio agli aspetti più prettamente tecnico-informatici, è opportuno dedicare la dovuta attenzione anche alla descrizione, nei loro tratti essenziali, di alcune esperienze, nazionali ed internazionali, in materia di implementazione dei sistemi di FSE.

Con riferimento al quadrante italiano si illustreranno alcuni modelli di punta di FSE: quelli della regione Lombardia e della regione Emilia-Romagna. Si accennerà, poi, alle esperienze della Provincia di Treviso e soprattutto della Provincia autonoma di Trento, la quale si caratterizza per la peculiare attenzione che viene rivolta al ruolo del paziente-utente.

A livello internazionale si tratteggeranno le caratteristiche dei modelli maggiormente sviluppati nell'ambito dei Paesi che fanno parte dell'Unione europea, Francia e Inghilterra, i cui progetti di FSE sono già passati alla fase applicativa[89]. Si dedicherà spazio, da ultimo, all'esperienza statunitense, all'interno della quale si delinea chiara la

[88] Vi sono diverse versioni disponibili: la 2.xx e la 3.xx

[89] Progetti di FSE sono diffusi in quasi tutta Europa; molti però si trovano in una fase embrionale e non hanno ancora trovato concreta e completa applicazione.

volontà da parte del legislatore di incentivare l'adozione di questi innovativi approcci[90].

5.2 Esperienze nazionali

5.2.1 Regione Emilia-Romagna: Progetto SOLE

Il progetto SOLE, Sanità *On Line*, è un'iniziativa di *e-government* della regione Emilia Romagna e consiste in una rete informatica che mette in collegamento tra loro circa tremilaottocento medici di medicina generale (MMG) e pediatri di libera scelta (PLS) con tutte le strutture ed i medici specialisti delle aziende sanitarie della regione[91]. SOLE pone in condivisione le informazioni sanitarie di oltre quattro milioni di cittadini tra i diversi medici che li hanno in cura. Inoltre, il progetto si prefigge di riuscire a rendere disponibili sulla Rete, a vantaggio dell'assistito e del suo rapporto con il medico, la prenotazione di esami e visite, i referti, le dimissioni dall'ospedale.

I servizi offerti sono[92]:

- gestione del ciclo di vita prescrizione-refertazione specialistica ambulatoriale: ciò consente di amministrare i servizi per il controllo completo di tutto il ciclo informativo, dalla prescrizione al ritorno del referto;
- gestione degli eventi di ricovero-dimissione;

---

[90] Un interessante approfondimento sui sistemi sanitari inglese, canadese e statunitense, fornito di un'utile ricostruzione storica, in L.J. NELSON, *A Tale of Three Systems: a Comparative Overview of Health Care Reform in England, Canada, and The United States*, 37 *Cumb. L. Rev.* 513 (2006/2007).

[91] V. sito web: <http://www.progetto-sole.it/consultazione/home.php>. Per approfondimenti v. BUCCOLIERO, CACCIA, NASI, *e-He@lth*, cit., 46-47; MORUZZI, *Internet e Sanità*, cit., 296-313; ID., *Fascicolo sanitario elettronico personale e reti e-Health*, cit., 13-14.

[92] Informazioni tratte dal sito web: <http://www.progetto-sole.it/consultazione/ obiettivi.php>.

- gestione dei flussi amministrativi MMG-Aziende (anagrafe): tale servizio permette di amministrare i servizi per il controllo delle PPIP (prestazioni di particolare impegno professionale) e per l'aggiornamento delle anagrafiche degli assistiti (comprese la scelta-revoca);
- gestione del processo di «Assistenza Domiciliare Integrata» (ADI), la quale supporta i processi di attivazione di tali piani mediante il dialogo tra MMG-PLS e professionisti delle Aziende USL;
- gestione delle patologie croniche (es. diabete, scompenso cardiaco);
- «Indicizzazione Regionale degli Eventi Clinici» (IREC): questo al fine di creare una metodologia di gestione e di accesso a dati clinici e sanitari.

L'architettura di SOLE è tutta improntata all'interoperabilità dei dati sociosanitari mediante l'utilizzo di standard internazionali HL7, DICOM e di *Virtual Private Network* (VPN) su rete pubblica.

Agli operatori sanitari è stata distribuita una c.d. «carta operatore», con finalità di autenticazione al sistema e di firma dei documenti introdotti.

L'infrastruttura informatica è concepita in modo tale da avere diversi *data repository* dislocati nelle varie aziende: tale scelta è stata adottata alla luce della maggior facilità che essa garantisce in ordine alla soluzione di eventuali problemi di normalizzazione e standardizzazione delle informazioni.

5.2.2 Regione Lombardia: Progetto CRS-SISS

In Lombardia è attivo il Progetto CRS-SISS (Progetto Carta Regionale dei Servizi-Sistema Informativo Socio-Sanitario)[93], il quale

[93] V. il sito web: <http://www.crs.lombardia.it>. Per approfondimenti consulta BUCCOLIERO, CACCIA, NASI, *e-He@lth*, cit., 44-45; G. ANDREOLI, D. BELTRAMI, M. CARAMAZZA, S. CASCIOLI, M.G. MARINI, M. RAIMONDI (a cura di), *L'impatto dell'informatizzazione sulle aziende sanitarie lombarde e le relative implicazioni su*

in ambito sanitario consente l'interoperabilità e la cooperazione dei diversi sistemi informatici (Aziende Sanitarie Locali, Aziende ospedaliere, strutture sanitarie private accreditate a contratto, medici di medicina generale, farmacie, ecc.) nel trattamento dei dati sanitari dei cittadini, anche attraverso l'utilizzo del FSE. La regione Lombardia distribuisce ad ogni cittadino una carta dotata di un microprocessore, la «Carta Regionale dei Servizi» (CRS), la quale rappresenta lo strumento di riconoscimento del cittadino-paziente e di firma elettronica nell'ambito del Sistema Socio-Sanitario Regionale Lombardo. Essa consente, inoltre, di: accedere ai servizi della sanità via Internet; scegliere o modificare il nominativo del MMG; prenotare le visite specialistiche, in comodità e sicurezza, direttamente dal proprio computer; conoscere, in tempo reale, quando sono pronti i referti degli esami medici; consultare, in qualsiasi momento, il FSE per avere sempre sottomano la cronologia dei ricoveri e delle visite.

5.2.3 Provincia di Treviso: il «Libretto Sanitario Nazionale»

La ULSS 9 di Treviso ha attivato il «Libretto Sanitario Elettronico»: questo rappresenta un modello di erogazione dei servizi di certificazione sanitaria via web valido per l'intero SSN[94]. La procedura per accedere alle proprie informazioni sanitarie da parte dei cittadini trevigiani è semplice: basta collegarsi al sito di Poste Italiane[95], inserire codice fiscale e *password* e si ottiene la possibilità di accedere, previo abbonamento, al proprio Libretto Sanitario Elettronico. In tal modo, ognuno ha la possibilità non solo di scaricare, a poche ore dalla prestazione medica, il proprio referto, ma anche di visualizzare l'archivio storico della propria documentazione sanitaria, leggere, in un arco di tem-

formazione e addestramento degli operatori, in Rete: <http://www.istud.it/up_media/ricerche/equal_san.pdf>.

[94] V. sito web: <http://www.ulss.tv.it/magnoliaPublic/categorie/link-utili/ritiro-referti.html>.

[95] V. sito web: <www.postesalute.it>.

po prescelto, il diagramma dei valori selezionati e scaricare i propri dati sanitari in ogni luogo e in ogni momento. In un contesto di crescente mobilità, il Libretto Sanitario Elettronico, realizzato a Treviso, permette di avere, in caso di necessità, dati clinici importanti e fondamentali, di fornirli ai medici di altre regioni o nazioni, che potranno a loro volta, inserire, nel rispetto dei protocolli stabiliti, ulteriore documentazione clinica.

La collaborazione con Poste Italiane è cominciata nel 2007 sulla base dell'esperienza trevigiana nel progetto TeleMed-ESCAPE. Dopo due anni, il Libretto Sanitario Elettronico è diventato operativo.

5.2.4 Provincia autonoma di Trento: il progetto «Cartella Clinica del Cittadino – TreC»

Il sistema sanitario provinciale trentino sta ideando e sperimentando un modello integrato di innovazione e sviluppo che si caratterizza per il potenziamento e l'integrazione dei servizi informativi esistenti, lo sviluppo di progetti in ambito di telemedicina e *homecare*, il riassetto dei processi organizzativi e gestionali, il ripensamento e la riorganizzazione della produzione e della gestione dei «documenti» sanitari[96]. All'interno di queste linee d'intervento si colloca il progetto «TreC – Cartella Clinica del Cittadino», sviluppato dal Dipartimento Politiche Sanitarie, Dipartimento Innovazione, Ricerca e ICT della Provincia autonoma di Trento in sinergia e collaborazione con la Fondazione Bruno

[96] La descrizione del progetto TreC si basa sulle «Linee Guida in materia di trattamento di dati personali e sanitari nell'ambito del sistema Cartella Clinica del Cittadino (TreC)» - Descrizione delle misure previste per garantire la conformità del sistema TreC alle disposizioni del d.lgs. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali), versione finale 2 luglio 2010, curate da U. IZZO e P. GUARDA. Di seguito il *link* al sito web relativo a quella che potremmo definire la «base preinstallata» di questo progetto, cioè il sistema di condivisione degli eventi clinici tra professionisti già attivo nell'Azienda Provinciale per i Servizi Sanitari (APSS) chiamato «AMPERE»: <http://www.apss.tn.it/Public/ddw.aspx?n=49003&h=-2147442770>.

Kessler, il Dipartimento di Scienze Giuridiche ed il Dipartimento di Sociologia e Ricerca Sociale dell'Università di Trento, l'Azienda Provinciale per i Servizi Sanitari di Trento (APSS) e altre componenti del Servizio Sanitario Provinciale. Esso intende promuovere una piattaforma di servizi di *e-care* che supportino il cittadino nella gestione della propria salute e cura, nonché le istituzioni socio-sanitarie nell'erogazione di nuovi modelli di servizi. A differenza delle tradizionali piattaforme di gestione informatizzata dei dati sanitari, che, come quella presupposta dalle LG FSE, privilegiano il ruolo dei gestori del servizio sanitario e dedicano al paziente un ruolo tutto sommato marginale e limitato, la piattaforma TreC presenta un approccio innovativo, caratterizzato da una struttura che elegge il paziente a parte integrante del sistema di gestione delle informazioni idonee a rivelare il suo stato di salute. Secondo tale prospettiva, ogni interazione del paziente con il nuovo sistema di gestione dei dati medici può implicare – con una scelta ovviamente rimessa esclusivamente al cittadino-utente stesso – la creazione di nuovi dati, che in tal modo, venendo archiviati su un'infrastruttura predisposta e gestita dalla APSS, entrano nella titolarità di quest'ultima (si determina così la creazione di un *Personal Health Record* (PHR)).

TreC è concepito per realizzare esclusivamente una finalità di cura e di assistenza sanitaria a vantaggio dei pazienti interessati, che in piena libertà decidano di giovarsi dei benefici connessi a tale innovazione, onde incrementare qualità ed efficienza nell'erogazione e nella fruizione dell'assistenza socio-sanitaria garantita agli assistiti dal Sistema Sanitario Provinciale.

Il modello trentino consente all'assistito-interessato di fruire di un *repository* elettronico di dati sanitari che lo riguardano, dotato di elevate garanzie di sicurezza e accessibile via web mediante l'impiego di sistemi di *strong authentication*[97]. L'APSS è titolare esclusivo del

[97] Questo *repository* dedicato al cittadino è stato definito «isola di dati»: con tale termine si individua un nucleo di informazioni il cui trattamento, sebbene rientrante

trattamento posto in essere mediante TreC.

Il sistema consiste in una piattaforma di servizi accessibili via web e in un apparato di applicazioni per il consumo e la fruizione di questi servizi che interagiscono fra loro. Concepito per essere utilizzato esclusivamente in base ad un'esplicita e specifica manifestazione di consenso da parte del cittadino-assistito, TreC può essere impiegato da quest'ultimo sia per ottenere un supporto nella gestione della propria salute, sia per interfacciarsi con le varie strutture e gli operatori sanitari provinciali nell'ambito di ciò che concettualmente identifica un FSE. Di seguito i moduli in cui si compone il progetto TreC:

- «Libretto Sanitario Elettronico»: il sistema garantisce all'assistito-interessato l'accesso alla documentazione clinica che lo riguarda già presente nel Sistema Informativo Ospedaliero (SIO). In un momento successivo, che presupporrà l'emanazione di ulteriori provvedimenti di indirizzo, esso permetterà in una logica di FSE di interfacciarsi con altri *dossier* sanitari relativi al medesimo interessato di cui siano titolari altre strutture sanitarie o soggetti che operano sul territorio provinciale per erogare prestazioni sanitarie a favore dell'interessato stesso (ovvero strutture private accreditate, MMG/PLS). Referti, esami di laboratorio, lettere di dimissione ed altri documenti già presenti nel SIO in formato elettronico, che attualmente sono messi a disposizione in modalità cartacea, tramite TreC potranno essere sempre raggiungibili dall'utente-interessato attraverso l'interfaccia messa a sua disposizione sulla rete Internet.
- «Diario della Salute»: tramite l'interfaccia TreC gli assistiti potranno inserire dati relativi alle proprie condizioni di salute, per tenere traccia dell'evoluzione del proprio quadro patologico, specie nel caso di pazienti affetti da malattie croniche, o di una condizione di interesse (ad es. attività fisica e dieta), ovvero, più semplice-

nell'ambito del più generale *dossier* dell'APSS, è caratterizzato da una *ratio* diversa. Di questa nuova categoria e del perché della sua previsione si dirà meglio più avanti.

mente, al fine di tenere un quadro aggiornato dei medicinali assunti. Quando TreC potrà evolversi in una logica di FSE, i dati oggetto del diario della salute del cittadino potranno, a discrezione dell'interessato, essere condivisi con i medici di propria fiducia (vedi prossima funzione).

- TreC supporterà nuove forme di comunicazione con i medici e le istituzioni sanitarie: il sistema permetterà ai cittadini di interfacciarsi elettronicamente con gli operatori sanitari. A seconda delle esigenze, esso potrà essere, ad esempio, una piattaforma di comunicazione in tempo reale di parametri vitali per un monitoraggio da remoto, un sistema di messaggistica protetta con i propri medici o, ancora, un canale per ricevere informazioni personalizzate da parte delle istituzioni sanitarie. Lo stesso Diario della Salute, in una successiva implementazione, potrà essere condiviso con gli operatori sanitari che avranno in cura il paziente.

Il modello trentino è stato studiato per essere una piattaforma idonea ad evolversi nel tempo, per supportare esigenze specifiche. Tra queste, ad esempio, la possibilità di interfacciarsi con strumenti di auto misurazione domestici (es. bilance, glucometri, apparecchi per la misurazione della pressione, ecc.) per consentire all'operatore sanitario curante un monitoraggio remoto più efficace.

In TreC i dati presenti nel sistema sono sempre accompagnati dall'indicazione del soggetto responsabile della loro immissione; risulterà possibile distinguere tra dati generati dal cittadino e dati creati da operatori sanitari (questa differenziazione viene evidenziata in modo inequivocabile attraverso colori e pittogrammi).

Il sistema prevede più canali di interazione, come ad esempio *smartphone* o applicazioni web. TreC è infatti concepito per supportare un sistema di applicazioni eterogenee destinate ad agevolare il cittadino nella gestione della propria salute. Questi potrà scegliere la configurazione delle applicazioni che meglio si adatta alle proprie esigenze ed

abitudini di vita. In concreto questa caratteristica viene resa fruibile all'utente attraverso un portale web destinato a fungere da principale canale d'accesso al sistema per tutti i cittadini[98].

Il progetto si trova attualmente in fase di sperimentazione.

5.3 Esperienze estere

5.3.1 Francia

Come noto, lo Stato francese è caratterizzato da una forma amministrativa fortemente centralizzata. Dal 1982, comunque, ha cominciato a svilupparsi una tendenza orientata verso il decentramento, che ha portato alla delega di poteri alle regioni. La popolazione francese è di circa sessantadue milioni di abitanti. Il sistema sanitario è misto: strutture private e pubbliche coesistono. I pazienti scelgono i loro medici di medicina generale ed hanno un accesso libero ai diversi tipi di strutture ospedaliere[99].

---

[98] V. il sito web: <www.trec.trentinosalute.net>.

[99] Per approfondimenti sul sistema francese di sanità elettronica v. EHR IMPLEMENT, *WP5 – National reports of EHR implementation – France*, 28 maggio 2009, in Rete: <http://www.ehr-implement.eu/download.cfm?downloadfile=A684205D-1143-DEB7-74D3FF51299F09E6&typename=dmFile&fieldname=filename>; E-HEALTH ERA, *Fact sheet France*, marzo 2007, in Rete: <http://www.ehealth-era.org/database/documents/factsheets/France.pdf>; V. PEIGNÉ, *Il trattamento dei dati sanitari in Italia e Francia tra convergenze e divergenze*, in *Dir. dell'Internet*, 2008, 296; ID., *Verso il Fascicolo Sanitario Elettronico: presentazione della riforma francese*, cit.; M. GAGNEUX, *Pour un dossier Patient virtuel et partagé et une stratégie nationale des systèmes d'information de santé*, 23 aprile 2008, in Rete: <http://www.d-m-p.org/docs/Rapport_DMP_mission_Gagneux.pdf>; EUSER, *eHealth Country Brief: France*, 2005, in Rete: <http://www.euser-eu.org/eUSER_eHealthCountryBrief.asp?CaseID=2220&CaseTitleID=1061&MenuID=118>. Sulla legislazione francese in tema di protezione dei dati personali, v. C. SARTORETTI, *Contributo allo studio del diritto alla privacy nell'ordinamento costituzionale. Riflessioni sul modello francese*, Torino, 2008; L. GUERRINI, *Prime osservazioni in margine alla nuova legge francese sulla protezione dei dati personali*, in *Dir. informazione e informatica*, 2004, 645;

I progetti di sanità elettronica sono sviluppati attraverso diversi attori, sia a livello regionale che locale. A livello nazionale è stata realizzata una mappatura di tutte le iniziative presenti. Di seguito una rassegna di quelle di maggiore interesse.

Innanzitutto il sistema *SESAM-Vitale*, introdotto alla fine degli anni novanta: esso interconnette più di duecentoventitremila operatori sanitari al SSN, a beneficio di più di quarantotto milioni di assistiti maggiori di sedici anni di età. Il sistema si basa su tre elementi:

- *Carte Vitale*, una carta a microprocessore che contiene semplici informazioni di carattere amministrativo; sostituita successivamente dalla nuova *Vitale 2*;
- *Carte de Professionnel de Santé* (CPS), una *smart card* con microprocessore utilizzata dai medici di medicina generale, creata nel 1993 (potenziata poi attraverso l'*Ordonnances Juppé* dell'aprile del 1996, «organizzazione di una sicura infrastruttura elettronica per i sistemi informativi sanitari»); le funzionalità incluse sono: identificazione, autenticazione e firma elettronica del personale sanitario;
- *Réseau santé social* (RSS), la rete sanitaria atta a gestire i flussi di dati e ad incoraggiare la comunicazione tra operatori sanitari e fondi assicurativi sanitari.

Esiste poi un portale ufficiale della sanità, sviluppato sotto la direzione del Direttorato Generale della Sanità del Ministero, che ha come obiettivo principale quello di promuovere l'informazione da parte delle agenzie pubbliche con riferimento a temi di sanità pubblica[100].

A. BERNARD, *La protection de l'intimité par le droit privé. Éloge du ragot ou comment vices exposès engendrent vertu*, in CURRAP (a cura di), *Le for intérieur*, Parigi, 1995, 155, in Rete <http://www.u-picardie.fr/labo/curapp/revues/root/35/alain_bernard.pdf_4a081e8ad4544/alain_bernard.pdf>; M. BESSONE, G. GIACOBBE, *Il diritto alla riservatezza in Italia e in Francia: due esperienze a confronto*, Padova, 1988; W.J. WAGNER, *Development of the Theory of the Right to Privacy in France*, 1971 *Wash. U. L. Q.* 45 (1971); H.E. PERREAU, *Les droits de la personnalité*, in *Rev. trim. dr. civ.*, 1909, 501.

[100] V. il sito web: <www.sante.fr>.

Infine, diverse applicazioni e piattaforme nel campo della telemedicina sono già utilizzate in alcune esperienze regionali. A livello nazionale opera il *Dossier Médical Personnel* (DMP): questo rappresenta un ambizioso progetto avviato nel 2004 con la *loi* n. 2004-810 del 13 agosto 2004, relativa *all'Assurance maladie* (il DMP è previsto nell'art. L. 161-36-1 del *Code de la Sécurité Sociale*)[101]. La riforma non ha rispettato i termini previsti (1° luglio 2004) a causa della non ancora generalizzata informatizzazione dei professionisti sanitari e dell'ampiezza del progetto (che riguarda sessanta milioni di pazienti), che, ad oggi, risulta ancora parzialmente incompleto[102].

La finalità del trattamento di dati posta in essere dal DMP consiste (per legge) nell'assicurare un miglior coordinamento, qualità e continuità del servizio sanitario. Altra finalità, di carattere prettamente politico, è poi quella di ridurre la spesa sanitaria.

Il DMP rappresenta un'infrastruttura atta ad archiviare, potenzialmente, i dati sanitari di tutti i beneficiari del sistema assicurativo sanitario obbligatorio. Non si tratta però di un fascicolo dell'operatore sanitario, essendo sotto il diretto controllo del paziente.

Esso contiene:

- dati che permettono l'identificazione del paziente (nome, cognome, data di nascita, *login* per l'apertura e il funzionamento del *dossier*) ed informazioni che ne identificano il medico curante;

[101] V. il sito web: <http://www.d-m-p.org/index.php>.

[102] Il DMP risulta amministrato da tre principali agenzie: 1) il *Groupement d'Intérêt Public dossier médical personnel*, (GIP DMP), responsabile per la programmazione del progetto, la selezione dei soggetti coinvolti e dei fornitori del servizio; 2) la *Commission Nationale Informatique et Liberté* (CNIL), un organismo del governo adibito alla vigilanza in tema di libertà civili e protezione dei dati personali; 3) il *Groupement d'Intérêt pour la modernisation du système d'information hospitalier* (GIP MISH), il quale coordina a livello nazione la modernizzazione e l'implementazione di sistemi informativi per gli ospedali ed i pazienti al fine di assicurare il rispetto degli standard utilizzati a livello nazionale per l'interfaccia DMP.

- dati di medicina generale (storia clinica, archivio delle consultazioni specializzate, allergie, intolleranze, vaccinazioni, ecc.);
- dati relativi alle cure (risultati degli esami, resoconti degli atti preventivi e terapeutici, patologie in corso, trattamenti in corso, ecc.);
- dati utili per la prevenzione (fattori di rischio individuale, resoconti preventivi, ecc.);
- dati relativi a reperti clinici (radiografie, *scanner*).

L'inserimento di nuove informazioni, la loro modifica o eliminazione è vincolata al consenso del paziente. Gli operatori sanitari hanno accesso al sistema attraverso l'uso simultaneo di due *smart-card*: la CPS e la *Vitale* del detentore del DMP. I pazienti possono accedere al DMP via Internet attraverso il portale nazionale. Le informazioni sono immesse nel sistema dai soli operatori sanitari a ciò abilitati. Ogni singola informazione è datata e firmata, e il suo autore identificato. Vi è pure una particolare sezione dedicata alle eventuali informazioni che il paziente stesso volesse inserire circa la propria salute.

La conservazione dei dati avviene sotto il controllo del paziente il quale deve scegliere un apposito *service provider* chiamato *hébergeur*, il quale deve essere previamente accreditato attraverso una procedura presieduta da una speciale commissione. Il legame tra paziente ed *hébergeur* è regolato da un contratto di *hébergement* inquadrato rigorosamente dal legislatore (l'*hébergement* ha l'obbligo di garantire la sicurezza e la confidenzialità dei dati nel rispetto delle disposizioni della legge ed è tenuto, per di più, anche al segreto professionale).

Il legislatore francese ha previsto un sistema di incentivi economici per la creazione e l'uso del DMP. Il rimborso degli atti e delle prestazioni mediche da parte del sistema nazionale di sicurezza sociale è subordinato all'autorizzazione che il paziente dà per accedere e com-

pletare il DMP (libertà forzata, oggetto di critiche e di dubbi a livello costituzionale)[103].

Il paziente possessore del DMP beneficia di un accesso libero all'insieme dei dati in esso contenuti tramite Internet, anche senza l'intervento di un operatore sanitario. Egli ha anche a disposizione, se lo desidera, i *log* file del sistema, al fine di poter esattamente conoscere chi ha avuto accesso, quando e a quali dati. Il consenso del paziente rappresenta il requisito necessario all'accesso ed alla gestione del DMP (principio di autodeterminazione). Occorre comunque tenere in considerazione che, nei casi di emergenza vitale, è stata prevista una particolare procedura, chiamata *bris de glace* (rottura del vetro), che permette agli operatori sanitari di accedere al DMP quando vi è impossibilità per il paziente di prestare il consenso. Il controllo è assicurato *ex post*, in quanto il paziente può sempre sapere con esattezza chi ha avuto accesso, quando e perché.

Il paziente ha il diritto di modificare i dati non sanitari direttamente presso l'*hébergeur*. Egli non ha invece la capacità di modificare il contenuto medico del DMP (*rectius*, i dati inseriti e firmati dagli operatori sanitari).

Il paziente ha comunque il diritto di *masquage*, di mascheramento: esso consiste nella facoltà di riservare, anche solo temporaneamente, l'accesso ad alcune informazioni al solo professionista sanitario autore delle informazioni stesse. Tale diritto si adegua alla realtà della relazione medico-paziente e tiene conto del fatto che l'assistito rivela le informazioni al medico in maniera proporzionale al grado di fiducia in esso riposta: maggiore è la fiducia, più dettagliate sono le informazioni fornite. Tale possibilità presenta, però, aspetti critici: gli operatori sanitari potrebbero con difficoltà essere ritenuti responsabili per il fatto di non aver posto in essere la corretta procedura di cura se non erano stati

[103] Si v. PEIGNÉ, *Verso il Fascicolo Sanitario Elettronico: presentazione della riforma francese*, cit., 627.

messi nelle condizioni di sapere che i dati a cui loro avevano accesso erano incompleti. In effetti, a ben vedere, il diritto di *masquage* presenta alcuni limiti. I potenziali rischi sono di natura sanitaria, nel particolare caso in cui le informazioni più sensibili (quindi maggiormente suscettibili di essere nascoste) coincidano con quelle più importanti per la cura del paziente (specie se il mascheramento è posto in essere da un paziente non sufficientemente consapevole dei rischi).

Il legislatore francese ha rigorosamente delimitato il campo dell'autonomia del paziente, prevedendo a priori tabelle che stabiliscono per ogni tipo di dato sanitario e per ogni professionista sanitario, quali siano i soggetti abilitati a leggere e/o inserire nuovi dati.

A differenza del sistema tradizionale di fascicolo sanitario, in cui ogni medico o struttura creano e conservano un *dossier* medico su ogni paziente, il nuovo sistema di condivisione dell'informazione presuppone l'utilizzo e la compilazione da parte di tutti i professionisti autorizzati di un unico documento.

5.3.2 Inghilterra

La popolazione totale del Regno Unito ammonta a circa sessanta milioni di abitanti. Ognuno dei quattro «Stati» che lo compongono (Inghilterra, Scozia e Galles ed Irlanda del Nord) ha elaborato un proprio approccio allo sviluppo ed alla implementazione di un sistema di fascicolo sanitario elettronico. Noi prenderemo a riferimento solamente quello adottato in Inghilterra, in quanto più avanzato degli altri, rivolto ad un numero più elevato di persone (circa cinquanta milioni) e di maggior interesse ai nostri fini[104].

[104] In generale sul modello inglese di FSE si v. i seguenti approfondimenti: V. JONES, C. JOLLIES, *eHealth strategy and implementation activities in England*, Report in the framework of the eHealth ERA project, 7 June 2007, in Rete: <http://www.ehealth-era.org/database/documents/ERA_Reports/England_eHealth_ERA_Country_Report_final_07-06-2007.pdf>; EHR IMPLEMENT, *WP5 – National reports of EHR implementa-*

Il più importante programma governativo di sviluppo in campo sanitario è costituito dal *National Health Service Plan* (NHS *Plan*), il quale include progetti per l'incremento degli investimenti in *Information Technology*.

Il *Department of Health* è responsabile per lo sviluppo dei progetti a livello statale. Le *Strategic Health Authority* regionali sono, invece, adibite al coordinamento ed alla gestione delle *performance* relative all'implementazione del programma nazionale a livello di organismi locali.

Il *National Programme for IT* (NpfIT), avviato nel 2002, rappresenta uno dei più cospicui investimenti nel campo dei progetti di sanità pubblica elettronica al mondo e ha come obiettivo principale quello di fornire accesso alle informazioni del paziente ovunque ed in ogni momento questo fosse necessario. Il suo scopo dichiarato è quello di implementare un'infrastruttura integrata e un sistema informativo che possa coinvolgere tutte le organizzazioni e i soggetti operanti all'interno del NHS a partire dal 2010.

Questi i sotto-programmi di cui si compone il NpfIT:

---

tion – England, 31 marzo 2008, in Rete: <http://www.ehr-implement.eu/download.cfm?downloadfile=305DE7DF-1143-DEB7-748EFE58B8FA6D90&typename=dmFile&fieldname=filename>; EHEALTH ERA, *Fact sheets: England*, marzo 2007, in Rete: <http://www.ehealth-era.org/database/documents/factsheets/UK_England.pdf>; C.N. MCCUBBIN, *Legal and ethico-legal issues in e-healthcare research projects in the UK*, 62 *Social Science & Medicine* 2768 (2006); C.N. MCCUBBIN, *Legal and ethico-legal issues in e-healthcare research projects in the UK*, 62 *Social Science & Medicine* 2768 (2006); EUSER, *eHealth Country Brief: United Kingdom*, 2005, in Rete: <http://www.euser-eu.org/eUSER_eHealthCountryBrief.asp?CaseID=2228&CaseTitleID=1069&MenuID=118>;; L. NICHOLSON, *Electronic Health Records in the United Kingdom of Great Britain & Northern Ireland*, in Rete: <http://www.ifhro.org/docs/ElectronicHealthRecordsinUKFINAL.doc>; T. SALEEM, *Implementation of EHR/EPR in England: a model for developing countries*, in *Journal of Health Informatics in Developing Countries*, 2009, vol. 3, n. 1, 9, in Rete: <http://www.jhidc.org/index.php/jhidc/issue/view6>.

- *NHS Care Record Service* (NHS CRS): fascicolo sanitario elettronico, atto a migliorare lo scambio dei dati dei pazienti all'interno del NHS ed a fornire ai pazienti stessi accesso ai loro dati sanitari[105].
- *Choose and Book*: un servizio a livello nazionale che, per la prima volta, fornisce la possibilità di prenotare, scegliere la struttura, la data e l'ora di un appuntamento per una prestazione ospedaliera. Esso rivoluziona il tradizionale sistema di prenotazione. Diverse ricerche in tale settore hanno dimostrato che i pazienti desiderano esser coinvolti sempre di più nel processo decisionale e nella scelta dei loro processi di cura. La maggioranza dei pazienti a cui è stata offerta questa nuova possibilità ha reagito in maniera positiva. Dall'estate del 2004 il servizio *Choose and Book* è stato introdotto in tutta l'Inghilterra. Dal primo gennaio 2006 tutti i pazienti che necessitino della prenotazione di un appuntamento hanno la possibilità di scegliere tra almeno quattro fornitori del servizio.
- *Electronic Prescription Service* (sistema per la trasmissione elettronica delle prescrizioni mediche): esso garantisce la possibilità di generare, trasmettere e ricevere prescrizioni elettroniche. Le prescrizioni sono spedite telematicamente da colui il quale le ha compilate al fornitore (farmacista), e infine all'autorità statale per quanto riguarda il loro pagamento. Dal 2007, tutti gli MMG ed i farmacisti hanno accesso al sistema.
- «N3»: è il nome della *NHS National Network* la quale garantisce una sicura ed affidabile infrastruttura di rete che connette tutti gli organismi facenti parte dell'NHS inglese. Questa rete ad alta velocità evidentemente rappresenta un potenziamento di tutti gli altri servizi offerti dal NHS.

[105] Questo progetto verrà analizzato nel dettaglio nel prosieguo. V. il sito web: <http://www.nhscarerecords.nhs.uk>.

- *Picture Archiving and Communications System*: il servizio permette di immagazzinare elettronicamente e di visualizzare sullo schermo immagini radiografiche ad altissima definizione.

Il NHS CRS è oggetto di introduzione graduale in tutta l'Inghilterra. Il processo, che impiegherà più anni per il proprio sviluppo, è iniziato a partire dal 2007. Ciò significa che per fasi successive le organizzazioni del NHS registreranno via via tutte le informazioni sanitarie su infrastrutture digitali interconnesse tra di loro. Questo permetterà allo *staff* medico un più rapido accesso alle informazioni con una modalità sicura. I pazienti stessi avranno accesso alle loro informazioni sanitarie essenziali. Il NHS CRS sarà in grado di connettere più di trentamila medici di medicina generale e duecentosettanta strutture del servizio sanitario attraverso un unico e sicuro sistema nazionale. L'infrastruttura si compone di due elementi: i dati dettagliati (raccolti e conservati a livello locale) e il *Summary Care Record* (conservato a livello nazionale).

Col nuovo sistema coloro che hanno in cura un soggetto potranno avere accesso a quelle parti del fascicolo sanitario delle quali è stata consentita loro la visualizzazione.

La scelta se creare o meno un *Summary Care Record* è rimessa alla volontà del paziente, il quale ha tre possibilità per limitare l'accesso alla propria cartella:

- chiedere che alcune informazioni non vengano incluse;
- chiedere che il *Summary Care Record* sia creato, ma non sia reso accessibile ad alcuno, senza il proprio esplicito consenso, al di fuori del proprio medico (che l'ha redatto);
- chiedere che non sia creato del tutto.

Al momento questo *summary* è stato adottato solo nelle zone dove il progetto è stato attivato (*Early Adopter Areas*).

L'accesso a questa selezione essenziale di informazioni sanitarie è garantita al paziente attraverso un portale *on-line* chiamato *Heal-*

thSpace[106]. Per ora non vi sono progetti in atto volti a rendere possibile per il paziente l'accesso ad un più dettagliato livello dei propri dati sanitari contenuti nei fascicoli elettronici. Per far ciò, si dovrà ricorrere alle normali procedure di accesso così come stabilito dal *Data Protection Act*[107]. Il *Summary Care Record* diverrà disponibile non appena il proprio medico di medicina generale l'avrà caricato su *HealthSpace*.

Oltre a garantire l'accesso al *Summary Care Record*, creato da un operatore sanitario, il portale offre anche al paziente la possibilità di conservare le informazioni relative alla propria salute, consentendo, ad esempio, di registrare i valori pressori, il peso e l'alimentazione, sia quotidianamente che ad intervalli regolari. Il progetto è stato lanciato il 13 giugno 2007, ma alla fine di marzo del 2008 erano ancora solo poco meno di seicentoquindicimila i pazienti che avevano registrato il proprio profilo, a causa dei molti dubbi sollevati circa il rischio di violazione della privacy di cittadini[108].

5.3.3 Stati Uniti d'America

5.3.3.1 Premessa: stato d'avanzamento nell'implementazione di sistemi di sanità elettronica

Fino all'anno 2000, l'adozione di sistemi di EHR, e in generale di altre tecnologie digitali applicate all'ambito medico (*Health Information Technology* – HIT), era veramente minimale. Meno del 10% degli ospedali statunitensi aveva attuato un piano per le HIT[109], mentre solo il

[106] V. sito web: <www.healthspace.nhs.uk>.

[107] Come primo approfondimento della disciplina inglese in materia di protezione dei dati personali v. LLOYD, *Information technology law*, cit., 3-203.

[108] Cfr. M.R. KIDD, *Personal Electronic Health Records: MySpace or HealthSpace?*, BMJ 2008, in Rete: <http://www.bmj.com/cgi/content/extract/336/7652/1029>.

[109] Cfr. D.J. RINGOLD, J.P. SANTELL, P.J. SCHNEIDER, *ASHP National Survey of Pharmacy Practice in Acute Care Settings: Dispensing and Administration—1999*, 57 *American Journal of Health-System Pharmacy* 1759 (2000).

16% degli MMG americani utilizzava un EHR[110]. In un torno di tempo tutto sommato ristretto questa tendenza, però, è stata invertita. Se è vero, infatti, che nel periodo 2001-2004 solo nel 18% dei casi di cure ambulatoriali si utilizzavano sistemi di EHR, già nel 2005, il 25% dei medici si servivano, in tutto o in parte, di sistemi elettronici di cartelle sanitarie (EMR)[111].

I motivi più comuni tra i commentatori sulle ragioni di tale iniziale insuccesso nello sviluppo di progetti di EHR si ritrovano negli elevati costi di implementazione e mantenimento di sistemi di questo tipo e nella mancata percezione di evidenti benefici dovuti alla loro adozione in termini di innalzamento della qualità ed efficienza del servizio sanitario. Le lamentele più diffuse si concentrano sul fatto che questi sistemi non agevolerebbero il lavoro degli operatori sanitari, in quanto renderebbero più gravosa l'attività di redazione ed archiviazione della documentazione medica; non presenterebbero una spiccata ed evidente utilità con riferimento all'attività di supporto alle decisioni; mancherebbero, inoltre, piattaforme veramente innovative atte ad incorporare tali applicazioni[112].

A conferma di ciò, l'adozione di sistemi di EHR ha inizialmente riguardato solo organizzazioni sanitarie che presentavano sistemi fortemente integrati, in grado di internalizzare i vantaggi e di finanziare gli elevati investimenti iniziali e le successive spese di mantenimento. Occorre allora citare due esperienze che si pongono tra i primi tentativi di

---

[110] Cfr. D. JOHNSTON ET AL., *The Value of Computerize Provider Order Entry in Ambulatory Settings: Executive Preview*, Wellesley, MA, 2003.

[111] Cfr. J.A. LINDER, J. MA, D.W. BATES, B. MIDDLETON, R.S. STAFFORD, *Electronic Health Record Use and the Quality of Ambulatory Care in the United States*, 167 *Arch. Intern. Med.* 1400 (2007).

[112] Cfr. EXECUTIVE OFFICE OF THE PRESIDENT – PRESIDENT'S COUNCIL OF ADVISORS ON SCIENCE AND TECHNOLOGY, *Report to the president realizing the full potential of health information technology to improve healthcare for americans: the path forward*, December 2010, 25-28, in Rete: <http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-health-it-report.pdf>.

adozione di sistemi di EHR: quella del *Veterans Health Administration* (VHA) e del *Kaiser Permanente*[113].

L'architettura «VistA», di cui si è dotato il VHA, è stata da più parti riconosciuta come uno tra i più rilevanti modelli di sistema integrato di salute della popolazione, volto a fornire un servizio di alto livello grazie all'utilizzo di IT (si veda, ad esempio, il sistema elettronico di richiami e di misurazione delle prestazioni volto a migliorare il tasso di vaccinazioni contro la polmonite)[114]. VistA ha consentito di ridurre il numero di errori terapeutici all'interno della struttura, facendo registrare indici di incidenza di questi assai inferiori alla media nazionale[115]. La piattaforma è stata resa disponibile in *open source*, sebbene difetti della flessibilità propria di altri sistemi commerciali: al momento essa non si connette, infatti, facilmente a molti tra questi e specialmente ai sistemi di PHR. Altro punto debole è rappresentato dalla scarsa propensione a creare banche dati di facile consultazione. Un discendente di VistA, l'*Armed Forces Health Technology Application* (AHLTA), contiene le cartelle cliniche di quasi dieci milioni di militari e delle loro famiglie.

Il *Kaiser Permanente's HealthConnect system*, invece, si basa su un sistema tra i più comunemente utilizzati dai fornitori privati: l'*Epic* EHR[116]. L'infrastruttura collega gli otto milioni e seicentomila pazienti di *Kaiser Permanente*, in nove Stati e nel Distretto di Columbia, a quattordicimila medici in quattrocentotrentuno ambulatori e trentasei ospedali[117]. Il personale medico è in grado così di recuperare i dati

---

[113] *Ibidem*, 28-31.

[114] VistA è infatti risultato vincitore nel 2006 del premio *Innovations in American Government Award*: v. il sito web governativo: <http://www.innovations.va.gov>.

[115] EXECUTIVE OFFICE OF THE PRESIDENT - PRESIDENT'S COUNCIL OF ADVISORS ON SCIENCE AND TECHNOLOGY, *Report to the president realizing the full potential of health information technology to improve healthcare for americans: the path forward*, cit., 28-29.

[116] V. il sito web: <http://www.epic.com/>.

[117] Si v. R. KAHN, *Kaiser Permanente Completes Electronic Health Record Implementation*, 2010, in Rete: <http://xnet.kp.org/newscenter/pressreleases/nat/2010

di qualsiasi paziente che ha ricevuto una prestazione sanitaria all'interno della loro rete. *Kaiser* ha utilizzato il sistema per migliorare l'assistenza preventiva e la gestione della cura delle malattie croniche. Tra i tanti servizi offerti, ad esempio, gli specialisti sono avvisati se un paziente è in ritardo per lo *screening* di prevenzione (come la mammografia). Una caratteristica supplementare di *HealthConnect* è quella di consentire ai pazienti di accedere ai dati *on-line* e di comunicare con i medici utilizzando un servizio di messaggistica sicuro. Più di tre milioni di pazienti di Kaiser sono registrati per questa funzione ed il sistema riceve oltre centomila accessi al giorno[118].

Solo di recente *Kaiser* e VHA hanno iniziato a collaborare per condividere i dati su pazienti che usano entrambi i sistemi; gli sforzi finora sono limitati ad una sola zona geografica (San Diego). *Kaiser*, inoltre, sta esplorando ulteriori interazioni con scambi di informazione sanitaria in alcune regioni[119].

Da ultimo resta da rilevare come sul settore abbiano cominciato ad investire grosse aziende private che cercano di accaparrarsi il controllo di questo stimolante ed economicamente promettente nuovo mercato. Si veda, tra tutti, il caso dei giganti *Google*, con il suo *Google Health* – servizio basato sul web per la gestione delle cartelle sanitarie personali (PHR) –[120], e *Microsoft*, con *HealthVault*[121]. I rischi per la

/030310ehrcomplete.html>. Il *Kaiser Permanent* è un consorzio di gestione integrata dei servizi sanitari che ha sede ad Oakland in California; per maggiori dettagli v. sito web: <https://www.kaiserpermanente.org/>.

[118] Cfr. C. CHEN, D. GARRIDO, G. OKAWA, L. LIANG, *The Kaiser Permanente Electronic Health Record: Transforming and Streamlining Modalities of Care*, 28 *Health Affairs* 323 (2009).

[119] Si registrano anche altre esperienze quali quello della *Palo Alto Medical Foundation* (PAMF) ed il *Geisinger Health System*: v. EXECUTIVE OFFICE OF THE PRESIDENT – PRESIDENT'S COUNCIL OF ADVISORS ON SCIENCE AND TECHNOLOGY, *report to the president realizing the full potential of health information technology to improve healthcare for americans: the path forward*, cit., 30-31.

[120] V. il sito web: <https://www.google.com/health/>.

[121] V. il sito web: <http://www.healthvault.com/>.

privacy dei pazienti posti da queste iniziative promosse da aziende private, seppur già intuibili, sono ancora tutti da scoprire.

5.3.3.2 Incentivazione normativa dei sistemi di Electronic Health Record

Al fine di stimolare l'adozione di sistemi di EHR, il Presidente Obama ha firmato una legislazione *ad hoc*: l'*American Recovery and Reinvestment Act* (ARRA) del 2009. Con esso si prevede un investimento di ventisette miliardi di dollari al fine di promuovere la diffusione delle tecnologie digitali in ambito medico[122]. Fa parte di questo pacchetto normativo anche l'*Health Information Technology for Economic and Clinical Health Act* (HITECH)[123].

L'HITECH ha creato la figura del *National Coordinator for Health Information Technology* (ONC)[124], il quale ha il compito di aggiornare il *Federal Health IT Strategic Plan*, includendo in esso alcuni obiettivi fondamentali quali lo scambio elettronico e l'utilizzo delle informazioni sanitarie di tutti i cittadini americani entro il 2014[125]. Il Titolo IV della legge promette incentivi economici per quanti scelgano di utilizzare *certified* EHR, contemplando nel contempo una riduzione dei finanziamenti pubblici per quanti, invece, optassero di non farlo. L'HITECH *Act* cerca anche di favorire il fatto che sia il *Secretary of*

[122] Cfr. S. HOFFMAN, A. PODGURSKI, *Meaningful Use and Certification of Health Information Technology: What about Safety?*, in *Journal of Law, Medicine and Ethics, Forthcoming. Case Legal Studies*, Research Paper No. 2010-34, October 2010, in Rete: <http://ssrn.com/abstract=1697587>.

[123] Cfr. N.P. TERRY, *Certification and Meaningful Use: Reframing Adoption of Electronic Health Records as a Quality Imperative*, in *Indiana Journal of Health Law, Forthcoming. Saint Louis U. Legal Studies.* Research Paper No. 2010-29, October 2010, in Rete: <http://ssrn.com/abstract=1687658>.

[124] L'*Office of the National Coordinator for Health Information Technology* (ONC) è un'agenzia federale che si trova presso l'HHS.

[125] ARRA § 13101.

Health and Human Services (il corrispettivo – potremmo dire – del nostro Ministro della salute) a fissare standard volti a coordinare i piani di sviluppo di queste infrastrutture a livello nazionale.

Da un punto di vista finanziario, sul versante della sanità elettronica, il sopra citato ARRA stanzia circa trenta miliardi di dollari per il *Department of Health and Human Services* (HHS): circa ventisette miliardi per i *Centers for Medicare & Medicaid Services* (CMS) e due miliardi per l'ONC. Con questi strumenti il CMS si occuperà di finanziare il programma di incentivazione dei sistemi EHR, mentre l'ONC fornirà il coordinamento e la pianificazione, tra le altre cose finanziando iniziative statali e regionali, attraverso borse di studio o prestiti. Gli incentivi saranno corrisposti a medici non operanti all'interno di strutture ospedaliere (*eligible providers*) e ad ospedali[126]. Il programma di sovvenzioni coprirà il periodo 2011-16, con incentivi che andranno diminuendo dopo i primi due anni. A partire dal 2016, i soggetti beneficiari e gli ospedali che non riusciranno ad utilizzare qualificati sistemi di EHR (*meaningful purposes*) si vedranno ridurre i pagamenti da parte del CMS.

Il concetto di *meaningful use*, utilizzato come *discrimen* per l'ottenimento del finanziamento nella disciplina di settore, diviene cruciale all'interno del pacchetto di sovvenzioni. CMS, ONC ed i vari comitati consultivi di HIT hanno sviluppato una serie di regolamenti atti a chiarire e definire gli ambiti di tale clausola generale all'interno di un c.d. *meaningful use matrix*, i cui elementi sono: «obiettivi», «misurazioni» e «stadi»[127]. In tal modo si legano assieme i risultati che si pro-

[126] ARRA § 4101 e 4102.

[127] V. la pagina di approfondimento del *Center for Medicare and Medicaid Services* relativa al concetto di *Meaningful Use*, in Rete: <http://www.cms.gov/EHRIncentive Programs/30_Meaningful_Use.asp#BOOKMARK>.

pone di raggiungere il piano nazionale ad obiettivi predefiniti, strumenti che garantiscano il rispetto di questi ed alla tempistica per il progetto[128].

Le finalità a carattere generale perseguite dallo HITECH sono: (1) migliorare la qualità, la sicurezza e l'efficienza delle cure, nonché ridurre le disparità; (2) coinvolgere i pazienti e le famiglie nella loro cura; (3) incentivare la salute pubblica; (4) potenziare il coordinamento dell'assistenza, (5) promuovere la privacy e la sicurezza degli EHR[129].

Nell'ambito di questi risultati di carattere generale si pongono, quali sotto-categorie, i suddetti «obiettivi» (ad es. la capacità di elevare il livello di qualità del servizio), l'elemento legato alle «misurazioni» (dove sono stabiliti i criteri o parametri volti a segnalare i progressi che il sistema compie)[130], infine i tre «stadi» di implementazione del sistema: una prima fase a partire dal 2011, una seconda fase a partire dal 2013, ed una terza ed ultima a partire dal 2015.

Altro elemento importante è quello che riguarda la certificazione (*certification*) dell'adozione di un sistema di EHR che garantisca un *meaningful use*[131]. L'ONC ha emanato le regole che stabiliscono gli standard di riferimento ed un processo di certificazione temporanea per i primi risultati[132].

---

[128] B. BROWN, *The Definition of "Meaningful Use"*, in *Journal Health Care Compliance*, 2009, 45-46, 72.

[129] LAB LAW WEEKLY, *U.S. Department of Health and Human Services HHS; CMS and ONC issue Regulations Proposing a Definition of 'Meaningful Use' and Setting Standards for Electronic Health Record Incentive Program*, in *Lab Law Weekly*, January 15, 2010; BROWN, *The Definition of "Meaningful Use"*, cit.; C.M. DESROCHES, S.J. ROSENBAUM, *Meaningful Use of Health Information Technology in U.S. Hospitals*, *New England*, 362 *Journal of Medicine* 1153 (2010).

[130] HITECH § 495.6.

[131] Cfr. TERRY, *Certification and Meaningful Use*, cit., 11-14.

[132] V. in generale le informazioni contenute nel portale dell'ONC all'URL: <http://healthit.hhs.gov/portal/server.pt/community/standards_and_certification/1153/home/15755>, dove si legge: «Providers and patients must be confident that the electronic health information technology (health IT) products and systems they use are secure, can maintain data confidentially, can work with other systems to share information, and can perform a set of well-defined functions».

Mentre lo standard del *meaningful use* si applica ai fornitori del servizio che desiderino beneficiare dei finanziamenti erogati, il concetto di *certification* è da rapportarsi al tipo di tecnologia utilizzata[133]. La regola così stabilita fornisce ai produttori di piattaforme EHR le specifiche minime necessarie per poter ottenere la certificazione del sistema[134]. Queste prevedono: la capacità di registrare e tracciare i segnali vitali, il mantenimento di liste di farmaci, la possibilità di prevedere i risultati dei *test* di laboratorio, la capacità di generare elenchi di pazienti con specifiche condizioni cliniche, ecc.[135].

Sin dai tempi dell'amministrazione Bush era attivo un singolo organismo di certificazione, la *Certification Commission for Health Information Technology* (CCHIT)[136]. L'ONC ha, invece, deciso di prevedere diversi organismi qualificati, al fine di gestire meglio lo sviluppo progressivo dei progetti[137].

In conclusione, possiamo affermare che l'esperienza statunitense propone un sistema di incentivi economici che dovrebbero favorire la diffusione di modelli di gestione dei dati sanitari basati su piattaforme EHR a livello del SSN. Ciò per superare, come già evidenziato, gli altissimi costi iniziali di messa in opera di detti sistemi e le spese legate al loro mantenimento a fronte di non chiari e, ad oggi, non facilmente prevedibili vantaggi. Si tratta evidentemente di una scommessa che cerca di premiare i progetti maggiormente attenti alla cura dei cittadini

[133] OFFICE OF THE NATIONAL COORDINATOR FOR HEALTH INFORMATION TECHNOLOGY, *Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology*, 13 luglio 2010, in Rete: <http://www.ofr.gov> (*Certification Rule*); DEPARTMENT OF HEALTH AND HUMAN SERVICES, *Standards and Certification Criteria Final Rule: Fact Sheet*, in Rete: <http://healthit.hhs.gov>.

[134] 45 CFR 170.

[135] 45 CFR 170.302 (d, e, f, h, i).

[136] V. il sito web: <www.cchit.org>.

[137] V. Cfr. TERRY, *Certification and Meaningful Use*, cit., 13-14, dove si dettagliano le fasi di attuazione dei sistemi di EHR e le relative procedure per ottenere la certificazione richiesta.

(vedi lo standard del *meaningful use*), che lega poi ad una vera e propria certificazione la possibilità di poter continuare a godere degli incentivi economici (v. *certification*). Nel contesto dell'ordinamento statunitense il problema è stato affrontato con un approccio maggiormente condizionato da logiche economiche: solo nei prossimi anni si potrà valutare la bontà delle scelte compiute.

*5.3.3.3 Dati sanitari e privacy: l'*Health Insurance Portability and Accountability Act (HIPAA)

Il diritto alla privacy dei dati sanitari è regolato negli Stati Uniti da una miriade di differenti leggi e regolamenti. Oltre alle regole di origine di *common law*, i singoli Stati rappresentano il punto di riferimento della disciplina del settore: molti di essi hanno emanato diversi *statute* per regolare la materia. Il grado di protezione varia, però, sensibilmente da Stato a Stato.

A livello federale, la privacy dei dati sanitari è rimasta senza disciplina fino al 1996, quando il Congresso decise l'emanazione dell'*Health Insurance Portability and Accountability Act* (HIPAA). Alla luce di questo *statute* il *Department of Health and Human Services* promulgò, poi, alcuni regolamenti per meglio specificarne l'applicazione e al fine di fornire un livello minimo di protezione comune a tutti gli Stati, i quali, comunque, conservano la possibilità di emanare, a loro volta, leggi statali caratterizzate da un maggior grado di protezione e specificità.

L'HIPAA richiedeva agli operatori del settore medico-sanitario di passare all'uso di formati standardizzati (elettronici) per la condivisione delle informazioni mediche. Il Congresso aveva anche previsto l'emanazione di una normativa onnicomprensiva in materia di privacy dei dati sanitari entro l'estate del 1999. Allo spirare di questo termine senza che nulla fosse accaduto, il *Department of Health and Human*

Services (HHS) si assunse tale compito (ciò in forza di una specifica previsione dell'HIPAA che ne prevedeva la possibilità in caso di inerzia del legislatore federale). L'HHS lavorò alla redazione di una proposta di regolamentazione (pubblicata come 64 Reg. Fed. 59,917, Nov. 3, 1999), che ricevette più di cinquantamila commenti e mozioni di modifica. Nel dicembre del 2000 il Presidente Clinton annunciò la redazione del testo finale. Nell'aprile del 2001, però, fu il nuovo Presidente Bush a confermare l'entrata in vigore della normativa entro l'aprile del 2003[138].

La disciplina applicativa dell'HIPAA costituisce la prima completa regolamentazione a livello federale sulla protezione dei dati sanitari[139]. Essa costituisce un approccio normativo alquanto dettagliato alle

[138] Cfr. 67 Fed. Reg. 53, 182 (Aug. 14, 2002).

[139] Per descrivere sinteticamente gli aspetti chiave di questo provvedimento di larga portata, possiamo dire che la disciplina federale impone agli *health care provider*, cioè a coloro che forniscono servizi medici, agli *health plan*, cioè ai soggetti o ai gruppi che assicurano il pagamento delle spese mediche, nonché agli *health care clearinghouse*, cioè ai soggetti pubblici o privati che trattano dati medici per diverse finalità, di adottare una serie di misure organizzative e di protezione. In dottrina v. GARTEE, *Electronic Health Records*, cit., 371 ss.; E. HUTTON, D. BARRY, *Medical: Privacy Year in Review: Developments in HIPAA*, 2 *ISJLP* 347 (2006); T.J. WHITE, C.A. HOFFMANN, *The Privacy Standards Under the Health Insurance Portability and Accountability Act*, 106 *W. Va. L. Rev*. 709 (2004); S.A. TOVINO, *The Use and Disclosure of Protected Health Information for Research Under the HIPAA Privacy Rule*, 49 *S.D. L. Rev.* 1439 (2002); L.O. GOSTIN, J.G. HODGE, JR., *Personal Privacy and Common Goods: A Framework for Balancing Under the National Health Information Privacy Rule*, 86 *Minn. L. Rev*. 1439 (2002); P.D. JACOBSON, *Medical Records and HIPAA: Is It Too Late to Protect Privacy?*, 86 *Minn. L. Rev.* 1497 (2002); M. HATCH, *HIPAA: Commercial Interests Win Round Two*, 86 *Minn. L. Rev.* 1515 (2002); P.P. SWIRE, L.B. STEINFELD, *Security and Privacy After September 11: The Health Care Example*, 86 *Minn. L. Rev.* 101 (2002). Da parte di numerosi commentatori sono state sollevate critiche alle regole introdotte dall'HIPAA, soprattutto sulla base di studi empirico-applicativi. Uno dei maggiori punti dolenti evidenziati riguarda proprio la questione delle *covered entity* (*health plan*, *healt care clearinghouse* e *health care provider*): da queste rimarrebbero esclusi diversi soggetti che forniscono consigli e consulenze mediche o che vendono prodotti sanitari, e che in generale sono in possesso di informazioni sanitarie. La maggior parte degli incidenti di sicurezza che riguardano i dati sanitari provengono proprio da queste categorie.

specifiche misure tecniche da implementare per la protezione dei dati medici.

Il 13 febbraio del 2003 l'HHS annunciò, pertanto, l'adozione delle HIPAA *Security Final Rules*. Gli standard definitivi furono, poi, pubblicati sul *Federal Register* il 20 febbraio e prevedevano, come data per l'entrata in vigore, il 21 aprile 2003. La maggior parte dei soggetti sottoposti a questa disciplina hanno avuto comunque un biennio per adeguarsi (fino al 21 aprile 2005)[140].

Le *Security Rules* dell'HIPAA fanno parte delle *Privacy Rules* della stessa disposizione normativa ed il loro *enforcement* è demandato al CMS[141]. La *ratio* di tale intervento regolamentativo consiste nel garantire la confidenzialità, l'integrità e l'accessibilità dei dati sanitari in formato digitale tramite l'adozione di misure di sicurezza a livello amministrativo, fisico e tecnico.

Le regole tecniche sulla sicurezza sono ora più coerenti e compatibili con la disciplina prevista per la privacy e si applicano alle *protected health information* (PHI) raccolte ed archiviate in formato elettronico[142].

Per questo, è auspicabile un'interpretazione estensiva della categoria in oggetto, nel senso di includervi chiunque consapevolmente raccoglie o trasmette dati sanitari in formato elettronico per qualsiasi tipo di finalità, anche commerciale. Cfr. D.J. SOLOVE, *The Digital Person. Technology and Privacy in the Information Age*, New York, 2004, 70; S. HOFFMAN, A. PODGURSKI, *Securing the HIPAA Security Rule*, Case Research Paper Series in Legal Studies, Working Paper 06-26, December 2006, 5 ss., in Rete: <http://ssrn.com/abstract=953670>; SCHWARTZ, *Privacy and the Economics of Health Care Information*, cit.; L.O. GOSTIN, *Health Information Privacy*, 80 *Cornell L. Rev*. 451 (1995).

[140] Per maggiori informazioni sulle *Security Rules*, v. S. HOFFMAN, A. PODGURSKI, *Securing the HIPAA Security Rule*, in *Journal of Internet Law*, Spring 2007, in Rete: <http://ssrn.com/abstract=953670>. Il portale dell'HIPAA è in Rete: <http://www. hipaadvisory.com>.

[141] Sulle *Privacy Rules* v., in prima battuta, D.B. LORD, *The HIPAA privacy rule and medical records discovery (part two)*, 30 *AK Bar Rag* 6 (2006).

[142] Ciò, evidentemente, non elimina la necessità di implementare alcune misure di sicurezza per le PHI non digitalizzate, in quanto le HIPAA *Privacy Rules* (164.530(c))

Partendo dalla riconosciuta esigenza di standard non eccessivamente prescrittivi, in quanto l'incessante e vorticoso sviluppo tecnologico renderebbe la previsione di specifici requisiti tecnici obsoleta o, ancor peggio, danneggerebbe il progresso scientifico, l'HHS stabilì che gli standard sarebbero stati definiti in maniera non dettagliata e sarebbero dovuti essere graduali, flessibili e di regola raggiungibili attraverso vari e differenti approcci e tecnologie[143]. Il risultato finale offre, così, una regolamentazione di alto livello e risponde a ciò che un modello di *information security* deve essere in termini di adattabilità e flessibilità.

La disciplina in oggetto riconosce grande importanza all'analisi dei rischi interni alla struttura sanitaria e alla loro gestione, considerando tali aspetti come centrali per i processi organizzativi. Inoltre, il costo delle misure di sicurezza è stato annoverato tra i fattori più significativi da tenere in considerazione quando ci si trovi a dover prendere decisioni a tale riguardo.

La maggior parte degli standard di sicurezza incorpora specifiche tecniche per la loro attuazione, al fine di meglio descrivere le azioni ed i comportamenti che devono essere adottati per assicurare la conformità agli standard stessi. Solo tredici tra queste specifiche tecniche sono, però, obbligatorie; le restanti sono considerate *addressable*, nel senso che rappresentano diversi approcci possibili per raggiungere specifici standard e non vengono ritenute come necessarie a priori, in riferimento allo specifico soggetto sottoposto alla normativa ed al particolare tipo di trattamento in uso. La decisione sulla ragionevole ed appropriata natura di un'*addressable specification* rimane in capo al soggetto che deve adottarla e deve basarsi sull'analisi complessiva dell'ambiente tecnico e della struttura di sicurezza implementata nel caso specifico.

---

tuttora richiedono l'adozione di misure adeguate a prescindere dal tipo di formato utilizzato.

[143] Gli standard di sicurezza sono concepiti, almeno negli intenti dei loro ideatori, per essere *technology neutral* al fine di facilitare l'utilizzo delle più aggiornate e promettenti tecnologie che incontrano i bisogni delle differenti aziende ospedaliere.

Tale decisione può dipendere da diversi fattori, tra i quali l'analisi dei rischi, delle misure già adottate e del costo per implementare quelle nuove[144].

5.3.3.4 Privacy sanitaria e sistemi Electronic Health Record*: considerazioni di sintesi*

L'applicazione pratica delle regole stabilite dall'HIPAA e dalle relative *Security Rules* hanno sollevato numerosi dubbi e perplessità da parte dei commentatori che spesso hanno denunciato l'utilizzo di disposizioni eccessivamente brevi o addirittura oscure ed ambigue[145].

L'incompletezza delle previsioni contenute nelle *Security Rules* è probabilmente frutto di una scelta consapevole da parte dello HHS: quella di garantire ai soggetti obbligati all'adozione delle specifiche di sicurezza un elevato tasso di flessibilità nella valutazione delle misure più appropriate in relazione ai diversi scenari di implementazione[146].

In tal senso, un presunto difetto potrebbe, invece, rivelarsi un punto di forza, soprattutto se ci si pone in un'ottica comparatistica e si prendono in considerazione le difficoltà applicative che le regolamentazioni onnicomprensive, come quelle che emergono dall'analisi del modello europeo, presentano. La possibilità di modulare le soluzioni in rapporto alla realtà in cui si opera appare essere, infatti, quella maggiormente efficace per l'abbassamento del livello di rischio che incombe sui dati trattati.

---

[144] Alla luce di questo processo decisionale, occorre scegliere, poi, una fra tre diverse opzioni: 1) implementare le specifiche tecniche indicate; 2) implementare un misura di sicurezza alternativa per realizzare gli scopi della norma tecnica; 3) non implementare alcunché se la specifica tecnica indicata non è ritenuta ragionevole o appropriata e la norma tecnica può comunque essere adottata.

[145] Cfr. HOFFMAN, PODGURSKI, *Securing the HIPAA Security Rule*, cit., *passim*.

[146] Cfr. *ibidem*, 9 ss., dove si suggeriscono delle soluzioni ai problemi che i commentatori hanno evidenziato nell'applicazione dell'HIPAA e delle relative *Security Rules.*

Il sistema degli standard di sicurezza stabilito dall'HIPAA può costituire un valido modello di gestione dei dati sanitari, soprattutto in ragione della sua flessibilità la quale, prescrivendo un certo margine di discrezionalità nell'applicazione delle soluzioni prescritte dalla normativa, chiama i titolari delle procedure decisionali ad una più acuta consapevolezza dei rischi implicati nel trattamento informatico dei dati sanitari e ad una maggiore responsabilità nell'adozione delle soluzioni più idonee, in uno scenario per sua natura poliedrico e mutevole.

Tiriamo le fila degli approfondimenti svolti e descriviamo ora quale sia l'impatto delle regole giuridiche sui sistemi di EHR nel contesto giuridico statunitense.

Sussiste un fondamentale problema di carattere terminologico che oscura la comprensione sullo stato attuale delle informazioni sanitarie negli Stati Uniti[147]. I commentatori, i tribunali ed i legislatori stessi spesso fanno riferimento a concetti quali *health privacy issue* o *protective model*. In realtà, devono essere affrontate due diverse questioni che trovano articolazione, a loro volta, in due distinte dottrine giuridiche. Le informazioni sanitarie possono essere in pericolo o durante la loro raccolta o nel momento della loro divulgazione. La legge ha risposto a queste minacce separatamente, esprimendo due modelli distinti di privacy e di riservatezza.

L'approccio volto alla tutela della privacy pone limiti alla raccolta dei dati: potremmo, allora, per esempio, vietare qualsiasi raccolta in determinate circostanze o limitarla tramite una regola di proporzionalità (ad esempio, solo le informazioni necessarie per il trattamento). Quello, invece, basato sul concetto di riservatezza pone limiti alla divulgazione dei dati (ad esempio, fascicoli sanitari ospedalieri possono essere comunicati ai medici, ma non alle aziende farmaceutiche). Per

[147] Cfr. TERRY, FRANCIS, *Ensuring the Privacy and Confidentiality of Electronic Health Records*, cit., 708-719; J.G. HODGE ET AL., *Legal Issues Concerning Electronic Health Information: Privacy, Quality, and Liability*, 282 *JAMA* 1466 (1999).

esempio, il diritto di anonimato garantisce al paziente la tutela della privacy; mentre i sistemi di sicurezza creano l'ambiente tecnologico atto a limitare l'accesso alle informazioni per quei documenti protetti dalle regole sulla divulgazione delle informazioni.

I modelli di riservatezza e di privacy attualmente rinvenibili negli Stati Uniti (soprattutto se applicati ad un EHR) sono profilati e legati da diverse caratteristiche esistenti nel sistema. In primo luogo, va rilevato che la regolamentazione delle cartelle cliniche è principalmente opera della legge statale. In secondo luogo, va sottolineato che la legislazione in materia di riservatezza delle informazioni mediche è poco sviluppata. Inoltre il *common law* di origine statale e gli stessi *statute* sulla riservatezza in ambito medico forniscono poche soluzioni alle minacce poste da un sistema di EHR. Le più recenti disposizioni normative contenute nella regole sulla privacy dell'HIPAA hanno, poi, creato una sorta di parallelo codice federale sulla riservatezza, i cui difetti diventano molto più evidenti quando tutto ciò si applica ad un EHR. Infine, il diritto statunitense consente generalmente ai pazienti di rinunciare o di delegare praticamente l'intero controllo sulla raccolta e diffusione dei loro dati medici personali. Solo in circostanze molto limitate vi sono norme atte a rendere l'informazione sanitaria non trasferibile.

Per quanto riguarda più specificamente la disciplina di origine statale, occorre riaffermare che storicamente ad essa si vedeva riconosciuta la competenza in materia di cartelle cliniche. Di conseguenza le regole che governano il possesso dei documenti, l'accesso ad essi, gli obblighi di notifica e le norme di protezione dei dati variano a seconda dello Stato in cui si trova ad operare. Gli standard HIPAA sulla comunicazione dei dati rappresentano un'eccezione molto importante a questa regola generale, ma pur sempre un'eccezione incompleta ed imperfetta, poiché le disposizioni in materia di privacy (le c.d. *Privacy Provision*) sono soggette ad una clausola di salvaguardia che mantiene alcune prerogative statali.

Gli standard federali contenuti nell'HIPAA si applicano, come abbiamo visto, ad una gamma di *covered entity*, le quali trasmettono informazioni sanitarie in forma elettronica, ma non a tutti gli organismi che in generale gestiscono tali informazioni sanitarie[148]. Sono previste, poi, limitazioni in merito alla comunicazione delle informazioni sanitarie protette, comprese quelle riferibili alla salute passata, presente o futura, fisica o mentale o alle condizioni di un individuo, che lo identificano o possono identificarlo. La struttura ospedaliera può comunicare le informazioni sanitarie private (PHI) solo per quanto consentito dalle norme federali. L'obiettivo fondamentale dell'HIPAA è quello di richiedere che le strutture soggette alla sua applicazione diano al paziente informazioni adeguate riguardo alle loro policy in materia di privacy, insieme a quello di proteggere i sistemi di EHR dall'accesso esterno senza il consenso del paziente[149].

[148] 45 C.F.R § 160.102.

[149] 45 C.F.R. § 164.306. Cfr. M. ROTHSTEIN, *Currents in Contemporary Ethics: Research Privacy Under HIPAA and the Common Rule*, 33 *J.L. Med. & Ethic* 154 (2005). Purtroppo le norme federali hanno fatto ben poco per ottenere la fiducia del paziente o per favorire la partecipazione dei professionisti sanitari ai progetti di EHR. Ciò per una serie di fattori. In primo luogo, le regole si concentrano quasi esclusivamente sul processo di raccolta del consenso del paziente. Inoltre, una novella posta in essere durante l'amministrazione Bush ha privato il paziente di un'importante scelta nel momento iniziale del suo rapporto con il fornitore del servizio (v. 45 C.F.R. §§ 164.502, 164.506). La nuova disciplina elimina la necessità di ottenere qualsiasi tipo di consenso alla divulgazione per «usi di *routine*»; ossia il trattamento, il pagamento, o le operazioni di assistenza sanitaria. Prima il consenso era richiesto anche per questo tipo di operazioni. Le norme sulla privacy sono, poi, ancora troppo permissive per quanto riguarda gli usi secondari dei dati dei pazienti. Si prevedono, infatti, numerosi casi di utilizzo delle informazioni sanitarie al di fuori del consueto trattamento per finalità di cura o per scopi di carattere amministrativo. In troppe situazioni il consenso del paziente per usi secondari non è necessario, anche laddove si sarebbe invece dovuto vietare (vedi ad esempio, la vendita dei dati del paziente per il *marketing* farmaceutico). Infine, le norme federali non prevedono una regolamentazione per tutti i dati sanitari e per tutti gli utilizzatori di tali dati (cfr. ad esempio *Mathis*, 377 F. Supp. 2d, 645, dove l'FBI non è stata considerata una *covered entity*).

In conclusione, volendo pervenire ad assicurare un corretto livello di fiducia del paziente e degli operatori sanitari nei sistemi di EHR, occorre affrontare un problema di portata più generale, ovvero il fatto che le norme sono fatalmente imperfette perché carenti in tema di trasparenza e di chiarezza. Ciò che era richiesto alla disciplina federale era di porre in essere una garanzia giuridica per il paziente in ordine al controllo delle proprie informazioni sanitarie. Il sistema delle eccezioni avrebbe dovuto, dunque, essere concepito in maniera più restrittiva e strettamente legata al principio di proporzionalità, nonché profilato alle reali finalità di prevenzione e di cura proprie delle strutture sanitarie[150].

[150] Una delle caratteristiche più pervasive dell'approccio statunitense alla riservatezza ed alla privacy è rappresentata dal fatto che i pazienti possono rinunciare o delegare quasi tutti i controlli esistenti per la raccolta o la diffusione di informazioni sanitarie personali. Ciò è stato reso operativo in *common law* attraverso la dottrina della rinuncia (cfr. *Mull v. String*, 448 So. 2d 952 (Ala. 1984) e, negli *statute* statali, da apposite disposizioni di autorizzazione (cfr. ad esempio Cal.Civ. Code § 56.11 (West 1982 & Supp. 2006). Leggi statali che vietano l'uso di informazioni sanitarie in determinate circostanze rappresentano, invece, un'eccezione: ad es., molti Stati prevedono alcune limitazioni con riferimento all'uso delle informazioni genetiche in ambito di assicurazioni per malattia, mentre pochi le estendono anche alle assicurazioni per la vita e per invalidità. Cfr. Ala Code § 27-53-2(a) (LexisNexis 1998); Kan Stat. Ann. § 40-2259(b)(1) (2000); Minn. Stat. Ann. § 72°-139(3)(1) (West 2005). Le poche disposizioni sulla non trasferibilità potrebbero costituire un modello interessante, soprattutto in riferimento ai sistemi di EHR.

CAPITOLO II

IL QUADRO NORMATIVO ITALIANO

1. Le regole del Fascicolo Sanitario Elettronico nell'ordinamento italiano

Dopo aver delineato nel primo capitolo il contesto normativo nel quale si collocano le nuove esperienze volte all'informatizzazione del SSN e dopo aver analizzato le variabili tecnico-informatiche che le connotano, è il momento di affrontare i problemi che la concezione, l'implementazione e la gestione di un sistema di FSE innescano sul piano della protezione dei dati personali dei soggetti coinvolti.

Come abbiamo già ricordato sopra, a livello di legislatore europeo i punti di riferimento normativi sono rappresentati dalla Direttiva 95/46/Ce e dalla Direttiva 2002/58/Ce[1]. A livello nazionale, il testo di riferimento è costituito ovviamente dal Codice Privacy. Tali interventi normativi hanno dedicato al problema del trattamento dei dati sanitari una disciplina *ad hoc*.

Il Garante Privacy, alla luce delle spinte – provenienti anche da documenti e raccomandazioni approvati in contesti sovranazionali (come il «Documento di lavoro sul trattamento dei dati personali relativi alla salute contenuti nelle cartelle cliniche elettroniche (CCE)», adottato il 15 febbraio 2007 dal Gruppo di lavoro articolo 29 per la protezione dei dati personali; d'ora in avanti: Documento CCE Gruppo art. 29) – alla messa in opera di un sistema di FSE, il 5 marzo 2009 varava un provvedimento a carattere generale avente ad oggetto le «Linee guida

[1] Come modificata dalla già citata Dir. 2009/136/Ce.

in tema di fascicolo sanitario elettronico e di *dossier* sanitario», avviando contestualmente una consultazione pubblica al fine di ricevere osservazioni e commenti entro il 31 maggio 2009. Lo scopo della consultazione era quello di finalizzare questo momento di confronto istituzionale con gli *stakeholder* all'emanazione di un nuovo provvedimento che avrebbe dettato la cornice regolativa di riferimento per le future applicazioni di sanità elettronica in Italia. Il processo consultivo è poi culminato nell'emanazione da parte dell'Autorità Garante di un Provvedimento a carattere generale concernente «Linee guida in tema di Fascicolo Sanitario Elettronico (Fse) e di *dossier* sanitario - 16 luglio 2009» (LG FSE).

È evidente che la definizione giuridica di FSE nel contesto regolativo della protezione dei dati personali non può che rispecchiare una concezione della cura che il sistema sanitario nel suo complesso (sistema nel quale prendono posto con ruoli e responsabilità differenziate, ma sempre più integrate, soggetti pubblici e privati) si ripromette di perseguire[2].

[2] V. sull'argomento G. CIPRIANO, *La cartella clinica digitale*, in *Dir. sanitario moderno*, 2008, fasc. 1, 17; FROOMKIN, *Forced Sharing of Patient-Controlled Health Records*, cit.; TERRY, *Personal Health Records*, cit.; TERRY, FRANCIS, *Ensuring the Privacy and Confidentiality of Electronic Health Records*, cit.; M.A. HALL, *Property, Privacy and the Pursuit of Integrated Electronic Medical Records*, Legal Studies Paper No. 1334963, 2009, in Rete: <http://ssrn.com/abstract=1334963>, dove si trovano interessanti approfondimenti sulle teorie circa le regole di appartenenza dei dati sanitari, sull'approccio statunitense al problema e sulle positive esternalità di rete che l'implementazione di questi sistemi produce; A.M. FROOMKIN, *The New Health Information Architecture: Copying with the Privacy Implications of the Personal Health Records Revolution*, UM ELSI Group for Project HealthDesign (2008), in Rete: <http://www.projecthealthdesign.org/media/file/social-life-info-15.pdf>; L. POISSANT, J. PEREIRA, R. TAMBYLIN, Y. KAWASUMI, *The Impact of Electronic Health Records on Time Efficiency of Physicians and Nurses: A Systematic Review*, 12 *Journal of the American Medical Informatics Associations* 505 (2005); S. HOFFMAN, A. PODGURSKI, *In Sickness, Health, and Cyberspace: Protecting the Security of Electronic Private Health Information*, Working Paper 06-15, September 2006, in Rete: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=931069>; P.D. JACOBSON, *Medi-*

In tema di accesso ai dati sanitari da parte del cittadino si rinvengono interessanti indicazioni a livello comunitario. La Raccomandazione della Commissione del 2 luglio 2008 sull'interoperabilità transfrontaliera dei sistemi di cartelle cliniche elettroniche al «considerando» n. 3 così recita:

> I sistemi di cartelle cliniche elettroniche possono garantire una maggiore qualità e sicurezza delle informazioni sanitarie rispetto alle tradizionali cartelle cliniche. La loro interoperabilità dovrebbe facilitare l'accesso alle informazioni, e migliorare la qualità e la sicurezza dell'assistenza ai pazienti nell'intera Comunità fornendo loro e agli operatori sanitari informazioni aggiornate e pertinenti assicurando, al contempo, i massimi standard di tutela e riservatezza dei dati personali.

Sempre in detta raccomandazione si legge più avanti al punto 14, lett. h: [questo quadro giuridico è volto, in particolare, a:]

> garantire che i pazienti siano pienamente informati sulla natura dei dati e sulla struttura della cartella clinica elettronica che li contiene. I pazienti dovrebbero disporre di strumenti alternativi (convenzionali) per accedere ai propri dati personali inerenti alla salute. In tale contesto, è importante che le informazioni fornite ai diretti interessati utilizzino un linguaggio e un formato di facile comprensione, e siano comunicate in maniera adeguata a persone con particolari esigenze (ad esempio bambini o anziani).

---

cal Records and HIPAA: Is It Too Late to Protect Privacy?, 86 *Minn. L. Rev*. 1497 (2002); H.T. GREELY, *Trusted Systems and Medical Records: Lowering Expectations*, 52 *Stan. L. Rev*. 1585 (2000). Per maggiori dettagli con riferimento all'incorporazione dei principi giuridici propri del diritto alla privacy all'interno delle architetture digitali v. P. GUARDA, N. ZANNONE, *Towards the Development of Privacy-Aware Systems*, in *Information and Software Technology*, vol. 51, 2009, 337.

A livello nazionale altri documenti presentano chiari suggerimenti per la predisposizione di piattaforme FSE con riferimento al profilo dell'accesso da parte dell'utente interessato. Il TSE, nel documento rilasciato il 31 marzo 2005 «Una politica per la Sanità Elettronica», già indicava tra gli obiettivi prioritari dei servizi di sanità elettronica l'agevolazione dell'accesso ad essi tramite il potenziamento e la facilitazione della

> scelta dei cittadini attraverso l'interoperabilità tra i sistemi di prenotazione[3].

Nella «Strategia architetturale per la Sanità Elettronica» del 31 marzo 2006, sempre il TSE, indicando tra gli obiettivi dell'Infrastruttura di Sanità Elettronica la disponibilità delle informazioni cliniche, stabiliva che

> [l]'infrastruttura deve rendere disponibili le informazioni cliniche dell'assistito (la sua storia clinica) dove e quando queste sono clinicamente utili, da qualsiasi punto del territorio nazionale. Si dovrà cioè rendere disponibile all'assistito ed agli operatori sanitari autorizzati un Fascicolo Sanitario Elettronico (FSE), abbandonando progressivamente la gestione cartacea dell'attività clinica su scala nazionale[4].

A queste indicazioni si è aggiunta la presa di posizione del Garante, intervenuto con le «Linee guida in tema di referti *on-line*», anch'esso posto in consultazione pubblica e scaturente poi nelle definitive «Linee guida in tema di referti *on-line* 19 novembre 2009» (d'ora in avanti: LG Referti)[5].

---

[3] TSE, *Una politica per la Sanità Elettronica*, 31 marzo 2005, p. 2.2.

[4] TSE, *Strategia architetturale per la Sanità Elettronica*, 31 marzo 2006, p. 7, lett. a.

[5] Da ultimo anche le già citate «Linee guida sul fascicolo sanitario elettronico», proposte dal Ministero della Salute ed approvate dalla Conferenza Stato-Regioni, pre-

Le osservazioni che seguono si basano su una scelta di fondo: quella di analizzare la questione della refertazione *on-line* contestualmente a quella relativa alla gestione del FSE. Il Garante si è trovato, infatti, a distinguere le due problematiche sulla base dei diversi stadi di implementazione dei servizi di sanità elettronica a livello locale. In realtà, occorre ritenere che questi due momenti vadano affrontati avendo a mente un approccio unitario, in modo da governare il problema affrontato dalle LG Referti in seno alla logica di un sistema informativo concepito per la totalità dei dati inerenti lo stato di salute del paziente gestiti e legittimamente trattati dalle aziende sanitarie e dagli altri operatori sanitari.

Di seguito si compirà un'analisi ragionata e organica delle problematiche giuridiche connesse all'implementazione dei moderni sistemi di FSE. Per praticità espositiva si seguirà, laddove possibile, l'impostazione descrittiva propria delle LG FSE, per indicare alcune soluzioni pratiche, alla luce di valutazioni di carattere giuridico e tecnico, volte ad incorporare i principi e le regole inerenti alla disciplina dei dati personali nelle piattaforme digitali destinate a recepire il concetto di FSE. Questo rappresenterà il punto di partenza per un ragionamento di più ampio respiro che vorrà andare oltre nel capitolo successivo, ove si svolgeranno considerazioni a carattere più generale con riferimento ai punti nodali emersi nell'analisi di questi sistemi informativi calati nel più generale contesto del diritto dell'era digitale.

---

vedono un ruolo attivo del cittadino laddove suggeriscono la predisposizione di una sezione all'interno del FSE, chiamata «Taccuino personale del cittadino», pensata per contenere dati ed informazioni direttamente inseriti dall'utente (p. 16).

2. Aspetti problematici legati all'implementazione di un sistema di Fascicolo Sanitario Elettronico

2.1 Definizione ed ambito applicativo

Fino a poco tempo fa mancava nell'ordinamento italiano una definizione di FSE, sia a livello di normazione primaria che secondaria. Si faceva, allora, riferimento a quella proposta nel Documento CCE Gruppo art. 29, dove la «Cartella Clinica Elettronica» veniva indicata come

> una documentazione medica completa o documentazione analoga sullo stato di salute fisico e mentale, passato e presente, di un individuo, in forma elettronica e che consenta la pronta disponibilità di tali dati per cure mediche ed altri fini strettamente collegati[6].

Muovendo da tale punto di partenza, le LG FSE forniscono una propria descrizione del fenomeno in esame, definendo il FSE

> l'insieme dei diversi eventi clinici occorsi ad un individuo, messo in condivisione logica dai professionisti o organismi sanitari che assistono l'interessato, al fine di offrirgli un migliore processo di cura[7].

Alla luce della ricognizione svolta «sul campo» e delle esperienze già avviate sul territorio nazionale[8], si ritrova poi una sottocategorizzazione dei possibili strumenti utilizzabili per la gestione dei dati sanitari di un paziente. Si definisce, allora, «*dossier* sanitario» lo strumento

---

[6] Documento CCE Gruppo art. 29, 4.

[7] LG FSE, p. 1.5.

[8] In particolare l'esperienza lombarda, del progetto CRS-SISS, e quella della Regione Emilia Romagna del progetto SOLE, di cui si avrà modo di trattare.

> costituito presso un organismo sanitario in qualità di unico titolare del trattamento (ospedale o clinica privata) al cui interno operino più professionisti[9].

Le schede individuali del MMG e del PLS non sono, invece, *dossier* ai sensi delle LG FSE in quanto poste in essere da un singolo professionista, unico titolare del trattamento[10].

Si parla di FSE propriamente inteso quando si tratti di

> dati sanitari originati da diversi titolari del trattamento operanti più frequentemente, ma non esclusivamente, in un medesimo ambito territoriale (es., azienda sanitaria, laboratorio clinico privato operanti nella medesima regione o area vasta)[11].

Questa definizione fa subito comprendere come tratto caratterizzante dello strumento FSE sia la condivisione di informazioni archiviate da differenti titolari, le quali possono essere gestite in specifici *dossier* sanitari concepiti come insiemi di dati riconducibili ad una situazione di «monotitolarità».

Nell'ambito del provvedimento del Garante, il FSE è inteso esclusivamente come uno strumento di condivisione logica di dati e documenti tra organismi e professionisti sanitari. Nel primo testo delle LG FSE posto in consultazione, il paziente non era in alcun modo preso in considerazione, né come possibile destinatario dei dati così generati ed archiviati che lo riguardano, né come generatore diretto di informazioni sanitarie che sempre alla sua persona attengono. La conclusione trovava peraltro conferma in un altro passaggio delle Linee guida poste inizialmente in consultazione dove si leggeva:

---

[9] LG FSE, p. 2.4.

[10] Si sottolinea come in realtà, per semplicità, si sarebbe potuto riferirsi anche a queste banche dati come a dei *dossier*.

[11] LG FSE, p. 2.4.

> [l]a titolarità del trattamento dei dati personali effettuato tramite il Fse/dossier dovrebbe essere di regola riconosciuta alla struttura o organismo sanitario inteso nel suo complesso e presso cui sono state redatte le informazioni sanitarie (es. azienda sanitaria o ospedale) (art. 4, comma 1, lett. f) del Codice)[12].

Tale formula presupponeva ed esplicitava – trattando della titolarità dei dati contenuti nel FSE – l'idea che questo concetto nascesse per considerare solo informazioni redatte presso aziende sanitarie-ospedaliere ed, eventualmente (l'esemplificazione del Garante testualmente non lo dice, ma lo si può ragionevolmente supporre), presso il MMG o il PLS.

In realtà questa concezione, partendo dal presupposto che il flusso di dati che alimenta il FSE non possa essere generato direttamente dal paziente interessato, non rispecchia la reale politica sanitaria perseguita nel nostro Paese dalle istituzioni ministeriali e territoriali cui compete l'erogazione dei servizi sanitari. Come già abbiamo avuto modo di ricordare, lo stesso «Piano Sanitario Nazionale 2006-2008» individuava come obiettivo fondamentale quello di

> favorire le varie forme di partecipazione del cittadino, in particolare attraverso il coinvolgimento dei pazienti e delle associazioni dei familiari.

La mancanza è stata poi colmata nella versione finale delle LG FSE, laddove si fa menzione della possibilità di prevedere l'inserimento dei dati da parte del paziente stesso. Il testo recita:

> [i]l titolare del trattamento può, inoltre, prevedere che l'interessato possa inserire o ottenere l'inserimento – anche in appositi moduli e secondo degli standard, anche di sicurezza, definiti dal titolare – talu-

[12] Provv. a carattere generale Garante Privacy, *Linee guida in tema di fascicolo sanitario elettronico e di dossier sanitario - 5 marzo 2009*, p. 4.2.

> ne informazioni sanitarie (es. autovalutazioni, referti emessi da strutture sanitarie di altre regioni o Stati) o amministrativo sanitarie (es. appuntamenti medici, periodicità dei controlli prescritti) che riterrà più opportune. Tali informazioni devono essere distinguibili (da un punto di vista logico o organizzativo) da quelle inserite dagli operatori sanitari, in modo tale da rendere sempre evidente a chi accede la «paternità» dell'informazione, ovvero l'identità del soggetto che l'ha generata[13].

Ciò indubbiamente descrive una funzionalità accessoria e aggiuntiva rispetto all'impostazione, che potremmo definire «tradizionale», seguita in un primo momento dal Garante. Questa scelta è sicuramente in linea con un approccio che tende a coinvolgere il paziente nel processo di cura (anche in chiave preventiva), considerandolo attore principale nella gestione delle informazioni che lo riguardano: tutto questo grazie alle potenzialità che lo strumento informatico garantisce con riferimento a livelli più o meno complessi di interazione con i processi di trattamento dei dati. Tale aspetto riguarda il fatto che il paziente deve essere messo in condizione di alimentare il quadro informativo inerente alle proprie condizioni di salute; quadro che, al ricorrere di date circostanze, potrà essere utilizzato dagli operatori professionali tenuti ad interagire con la storia della sua salute per garantirgli le migliori cure possibili. L'insieme delle informazioni che il paziente fornirà al sistema può essere definito concettualmente un'«isola di dati». Con questa espressione si intende l'insieme dei dati sanitari trattati esclusivamente in forma elettronica, facente parte di un *dossier* sanitario ed oggetto di logiche di trattamento specifiche nell'ambito della medesima finalità che caratterizza il *dossier* sanitario stesso[14].

[13] LG FSE, p. 5.9, 5.10.

[14] L'esigenza di definire una nuova categoria rispetto a quelle già indicate dal Garante Privacy nelle sue LG FSE deriva dal fatto che essa permette di meglio raffigurare e delineare quella particolare tipologia di dati che all'interno del sistema di FSE viene dedicata e profilata sul paziente e posta sotto il suo diretto controllo.

Pertanto, è necessario non precludere (ma, anzi, prefigurare anche) a livello definitorio la possibilità che nel FSE sia fatta confluire un'isola dinamica di dati alimentata direttamente dal cittadino e, come tale, riconoscibile da parte degli operatori professionali che al sistema (ed alle informazioni in esso contenute) accedano dopo quell'inserimento. Con riferimento a questa possibilità, è opportuno evidenziare alcuni aspetti importanti al fine di assicurare che il sistema informativo sia conforme alla legalità descritta dal Codice Privacy. Lo scenario è il seguente. Il paziente interessato può immettere il dato che lo riguarda nella sua «isola di dati». Le informazioni così archiviate verrebbero ad essere gestite dall'Azienda sanitaria locale (ASL), per confluire nel più generale *dossier* che si trova nella titolarità di quest'ultima. L'ASL, infatti, fornisce l'infrastruttura informatica ed il servizio di cui si giova il cittadino. Infine, il MMG, ove a ciò autorizzato dal paziente all'atto di immissione, ed in quanto investito di una finalità di cura nei confronti del paziente, dovrebbe essere messo in condizione di accedere al dato che il paziente stesso ha versato (o caricato) nel sistema informativo del FSE.

2.2 Costituzione e finalità del Fascicolo Sanitario Elettronico

Non esiste a livello legislativo un obbligo di costituzione di un sistema di FSE da parte degli organismi sanitari. La sua introduzione è, quindi, da intendersi, ad oggi, come del tutto facoltativa. Ciò premesso, l'unico riferimento normativo a carattere generale sul tema è rappresentato dal d.lgs. 7 marzo 2005, n. 82 («Codice dell'amministrazione digitale»; d'ora in avanti CAD) per quanto concerne l'obbligo di assicurare la disponibilità, la gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione in modalità digitale[15].

[15] Il CAD è stato recentemente oggetto di modifica ed integrazioni da parte del d.lgs. 30 dicembre 2010, n. 235 «Modifiche ed integrazioni al decreto legislativo 7

In assenza di una specifica previsione che determini gli obiettivi che tale strumento deve perseguire, il Garante sottolinea come il FSE abbia quali esclusive finalità quelle di

> cura dell'interessato, ovvero [di] assicurare un migliore processo di cura dello stesso attraverso la ricostruzione di un insieme – di regola su base logica – il più possibile completo della cronistoria degli eventi di rilievo clinico occorsi a un interessato relativi a distinti interventi medici[16].

Risulta esclusa ogni altra possibile finalità collegata, ad esempio, ad attività di programmazione, gestione, controllo e valutazione dell'assistenza sanitaria[17]. Per il perseguimento di finalità amministrative connesse all'erogazione della prestazione sanitaria richiesta – vedi ad es. prenotazione e pagamento di una prestazione – le LG FSE richiedono di strutturare il sistema separando i dati amministrativi dalle informazioni sanitarie, prevedendo, così, profili diversi di abilitazione in

---

marzo 2005, n. 82, recante Codice dell'amministrazione digitale, a norma dell'articolo 33 della legge 18 giugno 2009, n. 69». Per approfondimenti sul CAD si v., *ex plurimis*, F. FERRARI, *Il codice dell'amministrazione digitale e le norme dedicate al documento informatico*, in *Riv. dir. proc*., 2007, 415; M. GUERNELLI, *Il "Codice dell'amministrazione digitale" modificato*, in *Studium iuris*, 2006, 1399; ID., *Riflessi civilistici del "Codice dell'amministrazione digitale"*, *ibidem*, 787; C. SAFFIOTI, *Il Codice dell'amministrazione digitale è in vigore. Conoscere uno strumento che coinvolge la pubblica amministrazione, i cittadini e le imprese*, in *L'Amministrazione italiana*, 2006, fasc. 6, 887; E. CARLONI, *Codice dell'amministrazione digitale - Commento al d.lgs. 7 marzo 2005 n. 82*, Rimini, 2005; G. CASSANO, C. GIURDANELLA (a cura di), *Il codice della pubblica amministrazione digitale - Commentario al d.lgs. n. 82 del 7 marzo 2005*, Milano, 2005; C. ERCOLANO, *Codice dell'amministrazione digitale*, in *Nuovo dir*., 2005, 554; I. D'ELIA, M. PIETRANGELO, *Il Codice dell'amministrazione digitale nel processo di semplificazione normativa: genesi e criticità*, in *Informatica e dir*., 2005, 9; E. DE GIOVANNI, *Il "Codice dell'amministrazione digitale": prime impressioni*, in *Dir. dell'Internet*, 2005, 226.

[16] LG FSE, p. 2.8.

[17] *Ibidem*, p. 2.9.

funzione della differente tipologia di operazioni consentite agli attori del sistema[18].

Le eventuali future utilizzazioni del FSE per fini di ricerca scientifica, epidemiologica o statistica dovranno avvenire in conformità con la normativa di settore ed essere oggetto di preventiva e specifica attenzione (deve peraltro ricordarsi che la notificazione che le strutture sanitarie hanno già provveduto ad effettuare prevede spesso, tra le finalità di trattamento, sia le indagini epidemiologiche che la ricerca medica e biomedica)[19].

2.3 Principio di autodeterminazione

Il principio che deve caratterizzare l'operabilità della struttura informativa di un FSE è quello dell'autodeterminazione (artt. 75 e ss. Codice Privacy)[20]. Esso incontra la sua prima consacrazione nell'art. 32 cost. il quale così sancisce:

> La Repubblica tutela la salute come fondamentale diritto dell'individuo e interesse della collettività, e garantisce cure gratuite

[18] *Ibidem*, p. 2.10.

[19] *Ibidem*, p. 2.11. V. nel prossimo capitolo il paragrafo di approfondimento sul rapporto tra FSE e biobanche di ricerca.

[20] Il principio di autodeterminazione rappresenta l'essenza stessa del consenso. Nei moderni ordinamenti democratici si assiste ad una tendenza che porta ad una sempre maggiore valorizzazione della libertà del soggetto di autodeterminarsi con riferimento alla gestione dei propri beni e diritti. Sul principio di autodeterminazione in ambito medico v., in prima battuta, L. STILIO, *Il diritto all'autodeterminazione informativa: genesi storica di un diritto fondamentale dell'homo tecnologicus*, in *Nuovo dir*., 2002, 19; L. COSENTINI, *La relazione medico-paziente: rapporto tra dovere di cura e autodeterminazione della persona destinataria della cura. Indisponibilità del diritto alla salute*. Nota a Decr. Trib. Modena 14 maggio 2009, in *Giur. mer*., 2009, 2697; A. PINNA, *Autodeterminazione e consenso: da regola per i trattamenti sanitari a principio generale*, in *Contratto e imp*., 2006, 598. Il prof. Rodotà si riferisce a tale principio come «autodeterminazione e sovranità su di sé»: S. RODOTÀ, *Intervista su privacy e libertà*, (a cura di P. CONTI), Roma, 2005.

> agli indigenti. Nessuno può essere obbligato a un determinato trattamento sanitario se non per disposizione di legge. La legge non può in ogni caso violare i limiti imposti dal rispetto della persona umana.

Tale principio trova conferma e specificazione nell'art. 33 della legge 23 dicembre 1978, n. 833, istitutiva del SSN: qui si stabilisce, infatti, che gli accertamenti ed i trattamenti sanitari sono di norma volontari e che, qualora previsti, i trattamenti sanitari obbligatori devono comunque rispettare la dignità della persona, i diritti civili e politici, compreso, per quanto possibile, il diritto alla libera scelta del medico e del luogo di cura. In tal senso si veda anche la Convenzione di Oviedo («Convenzione per la protezione dei diritti dell'uomo e della dignità dell'essere umano nei confronti delle applicazioni della biologia e della medicina: Convenzione sui diritti dell'uomo e la biomedicina») adottata a Nizza il 7 dicembre 2000: ivi all'art. 5 si legge, quale norma generale, che

> un trattamento sanitario può essere praticato solo se la persona interessata abbia prestato il proprio consenso libero e informato. Tale persona riceve preliminarmente informazioni adeguate sulle finalità e sulla natura del trattamento nonché sulle sue conseguenze e i suoi rischi. La persona interessata può, in qualsiasi momento, revocare liberamente il proprio consenso.

In ambito sanitario è probabilmente da escludere un'interpretazione troppo restrittiva di tale importante principio in grado di determinare qualche difficoltà operazionale da parte dei soggetti che garantiscono e forniscono il servizio sanitario. I benefici di un sistema di FSE, infatti, non sono solo individuali, ma anche e soprattutto collettivi: migliore efficienza della cura corrisponde anche ad un risparmio di costi.

Da un punto di vista più prettamente tecnico, il richiamo a tale principio obbliga a dover considerare il fatto che l'interessato abbia la facoltà di scegliere, in piena libertà, se costituire o meno un FSE, senza

che tale scelta infici in alcun modo l'accesso da parte sua alle prestazioni del SSN, né abbia conseguenze penalizzanti sulla possibilità di usufruire delle prestazioni mediche. Esso impone anche di garantire la possibilità che i dati sanitari restino a disposizione del solo professionista-organismo sanitario che li ha redatti, senza doverli necessariamente includere nel FSE, e comunque impedendone la comunicazione ad altri attori del sistema[21]. Resta tuttavia salva la facoltà della struttura di comunicare all'utente che rifiuti di conferire i propri dati al FSE – fermo restando la garanzia circa l'erogazione dei livelli di assistenza inderogabili garantiti agli utenti del SSN – che tale rifiuto implicherà per lui l'esclusione dai vantaggi legati all'operatività del FSE all'interno del processo di cura (vantaggi che potranno essere oggetto di illustrazione all'atto della richiesta del consenso al trattamento informatizzato).

Il corretto declinarsi del principio di autodeterminazione nel contesto di una piattaforma digitale impone un bilanciamento tra gli interessi coinvolti: l'esigenza del paziente ad avere un controllo quanto più pregnante possibile sui propri dati, specialmente con riguardo ai soggetti che possono venirne a conoscenza, non può realizzarsi in una sorta di tirannia del singolo a danno dell'interesse superindividuale a implementare e gestire un SSN efficiente.

I modelli che si basano su infrastrutture PHR rappresentano certamente la realizzazione più elevata allo stato dell'arte di tale principio nel contesto dei sistemi di FSE. Si tratta di un principio che va applicato in modo tale da non pregiudicare il regolare svolgimento dell'attività medica, diagnostica e curativa, e da riconoscere in *bit* le diverse responsabilità che sulla gestione dei dati sanitari incombono, in

[21] Il legislatore francese ha previsto una sorta di incentivo economico per la creazione e per l'uso del *Dossier Médical Personnel*. Pur lasciando appunto libera la scelta di costituire o meno un sistema di FSE, è stato previsto che il rimborso degli atti e prestazioni mediche dalla sicurezza sociale sia subordinato all'autorizzazione che dà il paziente ai professionisti per accedere e per completarlo (v. art. L. 161-36-2 *Code de la Sécurité Sociale*).

special modo quella del medico. Argomentare diversamente potrebbe significare livellare pericolosamente una gerarchia curativa che, innata nel rapporto medico-paziente, pur nel rispetto dell'autonomia – ora anche informazionale – del secondo, garantisce, da sempre, il corretto svolgersi della prestazione medica.

2.4 Oscuramento dei dati

Il principio di autodeterminazione impone anche che all'interessato sia lasciata la libertà di non far confluire nel FSE alcune informazioni sanitarie relative a singoli eventi clinici, soprattutto nel caso dei c.d. dati «supersensibili». La struttura informativa dovrebbe prevedere un sistema di «oscuramento» dell'evento clinico – sempre revocabile – volto a garantire che almeno in prima battuta tutti i soggetti abilitati all'accesso non possano venire automaticamente a conoscenza non solo del dato oscurato, ma anche del fatto che l'interessato abbia esercitato l'opzione di oscurare il dato stesso (c.d. «oscuramento dell'oscuramento»)[22].

La modularizzazione nell'inserimento delle informazioni sanitarie all'interno del sistema di FSE e la scelta dei livelli di condivisione dei dati così inseriti presenta problemi di non poco momento. La scelta di oscurare o meno determinate informazioni contrasta con le modalità di implementazione di strutture «simil-FSE» che già si ritrovano nelle esperienze regionali e provinciali. Una soluzione pratica potrebbe essere quella di prevedere due categorie di «dati oscurati»: una relativa a

[22] LG FSE, p. 3.11, 3.12. Nel modello francese si parla di diritto di *masquage*, che consiste nella facoltà di riservare, anche solo temporaneamente, l'accesso ad alcune informazioni al solo professionista sanitario autore di queste. Cfr. V. PEIGNÉ, *Verso il Fascicolo Sanitario Elettronico: presentazione della riforma francese*, in *Dir. dell'Internet*, 2008, 296; P.L. FAGNIEZ, *Le masquage d'information par le patient dans son DMP, Rapport au ministre de la santé et des solidarités, 30 janvier 2007*, in Rete: <http://www.sante.gouv.fr/htm/actu/fagniez_dmp/rapport.pdf>.

quelli completamente oscurati, cioè a quelle informazioni per le quali il paziente chiede esplicitamente il non inserimento all'interno del sistema; una seconda relativa a quei dati che potrebbero essere raccolti in una sezione per così dire riservata, il cui accesso sia regolato direttamente dal paziente-interessato. Tutto questo deve trovare esplicazione nell'informativa fornita al momento della richiesta del consenso generale.

2.5 Problemi di titolarità del trattamento e regime di responsabilità per i dati inseriti

2.5.1 Titolarità e co-titolarità del trattamento dei dati personali

La normativa sulla protezione dei dati personali è caratterizzata da un approccio sicuramente iper-regolativo: vi sono, infatti, numerosi principi da seguire nel trattamento dei dati, misure di sicurezza da implementare, informative da predisporre, consensi da ottenere. Tali incombenze ricadono su soggetti responsabili della raccolta e del trattamento dei dati stessi. Quali sono, allora, gli attori della privacy dei dati sanitari? Su quali soggetti grava il carico che la normativa prevede? La questione si complica nel contesto digitalizzato, nel quale ai soggetti che direttamente gestiscono le banche dati e l'infrastruttura informatica si accompagnano enti ed istituzioni che regolano e governano lo svolgersi dell'attività sanitaria e dei servizi offerti e sui quali si basa l'architettura del sistema.

Nell'ambito della disciplina degli attori del trattamento dei dati, il Codice Privacy presenta un'impostazione più organica e della disciplina precedente, contenuta nella legge 31 dicembre 1996, n. 675 (Tutela delle persone e di altri soggetti rispetto al trattamento dei dati perso-

nali), che recepisce le numerose indicazioni che sia la dottrina che il Garante avevano fornito negli anni[23].

Ai sensi dell'art. 4, co. 1, lett. f, del Codice Privacy il titolare del trattamento è

> la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza[24].

Al titolare spetta, quindi, il compito di organizzare l'intero processo di trattamento di dati. Proprio per questo esso risulta essere il principale destinatario degli obblighi di responsabilità e delle sanzioni previste dalla normativa sul trattamento dei dati personali[25].

---

[23] Per approfondimenti v. F. GARRI, *I soggetti che effettuano il trattamento: il titolare, il responsabile e l'incaricato*, in G. SANTANIELLO (a cura di), *La protezione dei dati personali*, in G. SANTANIELLO (diretto da), *Trattato di diritto amministrativo*, vol. XXXVI, Padova, 2005, 131-166; C. DI COCCO, *Soggetti che effettuano il trattamento (Parte I – Titolo IV)*, in MONDUCCI, SARTOR (a cura di), *Il codice in materia di protezione dei dati personali*, cit., 119-156; P. PERRI, *Privacy, diritto e sicurezza informatica*, Milano, 2007, 12-25; BIANCA, BUSNELLI (a cura di), *La protezione dei dati personali*, cit., art. 28, 648-651 (commento di P.M. VECCHI), art. 29, 652-664 (con commento di M.G. MANGIA), art. 30, 665-681 (con commento di V. GAGLIARDI); S. MELCHIONNA, *I principi generali*, in R. ACCIAI (a cura di), *Il diritto alla protezione dei dati personali. La disciplina sulla privacy alla luce del nuovo Codice*, Santarcangelo di Romagna, 2004, 57-66; S. ORLANDI, *Gli adempimenti per i titolari dei trattamenti*, in ACCIAI (a cura di), *Il diritto alla protezione dei dati* personali, cit., 181-228.

[24] L'art. 2, lett. d, della Direttiva 95/46/Ce parla, invece, di «responsabile del trattamento», riferendosi al «titolare» nella versione italiana, e lo definisce come: «la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che, da solo o insieme ad altri, determina le finalità e gli strumenti del trattamento di dati personali».

[25] Cfr. GARRI, *I soggetti che effettuano il trattamento: il titolare, il responsabile e l'incaricato*, cit., 134-135.

La definizione di titolare del trattamento adottata dal Codice rispecchia quella a suo tempo prevista dalla l. 675/1996, con alcune integrazioni[26]. Queste sono contenute nell'inciso relativo alla possibilità di prendere le decisioni concernenti gli elementi fondamentali del trattamento «anche unitamente ad altro», introducendo così sul piano normativo una innovazione rilevantissima con riferimento alle conseguenze giuridiche associabili ad una novella scandita in pochi caratteri a stampa: si legittima la co-titolarità sui dati personali dell'interessato da parte di più soggetti titolari di un medesimo trattamento. Viene, inoltre, precisato che sono di competenza del titolare anche le decisioni in merito agli strumenti utilizzati per il trattamento[27].

Il soggetto che assume le vesti di titolare deve necessariamente essere colui sul quale incombono le scelte nell'ambito delle attività materiali di trattamento relative alle tipologie di dati da raccogliere e registrare, alla quantità di dati da acquisire, ai tempi di conservazione degli stessi in relazione ai fini, alle fonti da cui attingere, agli aggiornamenti, ecc. Esso, inoltre, può non essere il gestore di una banca dati, bensì chiunque eserciti di fatto il controllo sui contenuti delle informazioni e sulle decisioni da adottare. La titolarità del trattamento così intesa può, quindi, risultare concettualmente separata dall'agire materiale sui dati e caratterizzarsi di una natura, invece, più tipicamente amministrativa[28].

In passato la determinazione della figura del titolare all'interno degli enti, fossero essi pubblici o privati, ha dato adito ad accese discussioni tra quanti la individuavano nella persona fisica legale rappresentante e chi – tesi maggioritaria – nella struttura o nell'organismo

[26] Art. 1, co. 2, lett. d, l. 675/1996: «la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono le decisioni in ordine alle finalità ed alle modalità del trattamento di dati personali, ivi compreso il profilo della sicurezza».

[27] Cfr. DI COCCO, *Soggetti che effettuano il trattamento (Parte I - Titolo IV)*, cit., 123-124.

[28] Cfr. GARRI, *I soggetti che effettuano il trattamento: il titolare, il responsabile e l'incaricato*, cit., 135.

stesso nel suo complesso e non nelle singole persone fisiche. L'art. 28 del Codice Privacy ha completamente chiarito la questione sposando quest'ultimo orientamento:

> Quando il trattamento è effettuato da una persona giuridica, da una pubblica amministrazione o da un qualsiasi altro ente, associazione od organismo, titolare del trattamento è l'entità nel suo complesso o l'unità od organismo periferico che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza[29].

L'aspetto qualificante della figura del titolare del trattamento è, pertanto, rappresentato dall'autonomia del suo potere decisionale in relazione agli scopi del trattamento, alle scelte operative, agli strumenti da utilizzare, ecc.

---

[29] Cfr. *ibidem,* 134-135, ove si evidenzia come un primo orientamento minoritario individuava il titolare del trattamento nel legale rappresentante dell'ente (v. R. IMPERIALI, R. IMPERIALI, *La tutela dei dati personali*, Milano, 1997, 79); la dottrina prevalente, invece, riteneva già prima dell'introduzione del Codice che titolare fosse la struttura o l'organismo nel suo complesso (v. G. BUTTARELLI, *Banche dati e tutela della riservatezza*, Miano, 1997, 170). Il Garante stesso aveva avuto modo di rilevare che interpretando diversamente, cioè restringendo l'ambito di applicazione della categoria in esame alle sole persone fisiche da individuare parte delle persone giuridiche, pubbliche amministrazioni o enti al proprio interno, sarebbe divenuta illogica la sequenza dei soggetti indicati nella stessa norma: di seguito alla «persona fisica» (titolare del trattamento) è infatti menzionata la persona giuridica, la persona fisica, l'ente, l'associazione o l'organismo titolare del trattamento (v. art. 4, co. 1, lett. f), Codice Privacy): cfr. Provv. Garante Privacy del 9 dicembre 1997, in *Cittadini e società dell'informazione*, *Bollettino*, n. 2, 1997, 38. Sul punto v. anche DI COCCO, *Soggetti che effettuano il trattamento (Parte I – Titolo IV)*, cit., 124-126; MELCHIONNA, *I principi generali*, 58-59. Si ricordi, infine, che ai sensi dell'art. 18, co. 2, Codice Privacy il trattamento di dati da parte di un soggetto pubblico è consentito «soltanto per lo svolgimento delle funzioni istituzionali»: si collega, così, direttamente la liceità del trattamento stesso al rispetto del principio di legalità (le funzioni istituzionali dovranno esser previste ed individuate da un'apposita disposizione normativa).

La c.d. «co-titolarità» si realizza, invece, nel caso in cui le scelte su finalità, modalità, strumenti e misure di sicurezza da adottare per il trattamento siano riferibili a più soggetti. Il nostro Codice riconosce tale possibilità, nonostante il testo della Direttiva 95/46/Ce sembri propendere per la scelta di un unico titolare[30]. Questo istituto rappresenta uno snodo cruciale nella predisposizione di una struttura informatizzata volta alla gestione di dati sanitari. La condizione oggettiva da cui desumere una situazione di co-titolarità è data dal fatto che diversi soggetti esercitano i poteri propri del titolare in maniera del tutto autonoma e con riguardo al medesimo trattamento[31].

Un'altra figura rilevante nell'ambito del trattamento dei dati personali è rappresentata dal «responsabile del trattamento» che l'art. 4, co. 1, lett. g, del Codice Privacy definisce come

[30] Cfr. FINOCCHIARO, *Il trattamento dei dati sanitari*, cit., 208 ss.; GARRI, *I soggetti che effettuano il trattamento: il titolare, il responsabile e l'incaricato*, 141 ss.; DI COCCO, *Soggetti che effettuano il trattamento (Parte I – Titolo IV)*, cit., 123-124. Il Codice Privacy sul punto recepisce l'orientamento dottrinale che nella vigenza della precedente l. 675/1996 riteneva incompatibile con lo stesso dettato normativo la possibilità che più soggetti fossero coinvolti nelle decisioni in merito al trattamento, con un unico soggetto qualificato come titolare, ritenendo che in un'ipotesi di tal sorta tutti i soggetti coinvolti assumessero di diritto la qualifica di co-titolari: ciò sul presupposto che una diversa interpretazione avrebbe potuto ingenerare fenomeni elusivi della responsabilità, con la scelta di possibili titolari di comodo: cfr. L. LAMBO, *La disciplina del trattamento dei dati personali: profili esegetici e comparatistici delle definizioni*, in PARDOLESI (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, cit., 102. La stessa linea interpretativa era stata del resto anticipata dal Garante: v. Garante Privacy, *Risposte-quesiti*, 10 giugno 1998, in *Boll*., 1998, n. 5, 36, ove si afferma «che particolari articolazioni centrali o periferiche dell'amministrazione possono essere considerate come distinti ed autonomi titolari del trattamento diversi dal Ministero come complessiva entità, nel solo caso in cui esse esercitino un potere realmente autonomo su particolari sfere di trattamenti, non condizionato dalle complessive scelte che interessano l'amministrazione nel suo complesso pur nella specificità dei compiti rimessi ad ogni amministrazione»; v. anche Garante Privacy, *Parere*, 9 dicembre 1997, in *Boll.*, 1997, n. 2, 44.

[31] Cfr. GARRI, *I soggetti che effettuano il trattamento: il titolare, il responsabile e l'incaricato*, cit., 142.

> la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento dei dati personali.

Si tratta di una figura facoltativa nel trattamento dei dati, individuata da parte del titolare, alla luce di considerazioni di carattere organizzativo tra i

> soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza[32].

Il ruolo del responsabile non è caratterizzato da una semplice dimensione organizzativa interna, bensì si estrinseca anche in rapporti con l'esterno. Tale evidenza esterna trova, infatti, piena giustificazione, oltre che per ragioni di trasparenza del trattamento stesso, anche per il ruolo svolto in concreto. Egli, infatti, può sia interagire direttamente con il Garante che, eventualità molto più ricorrente, con i soggetti direttamente interessati al trattamento, i cui diritti, riconosciuti ai sensi dell'art. 7, possono esser fatti valere direttamente nei suoi confronti (oltre che, evidentemente, nei confronti del titolare)[33]. Nel più specifico ambito del trattamento dei dati sanitari, anche il responsabile può auto-

[32] Art. 29, co. 2, Codice Privacy. Cfr. *ibidem*, 145; DI COCCO, *Soggetti che effettuano il trattamento (Parte I – Titolo IV)*, cit., 125-129; BIANCA, BUSNELLI (a cura di), *La protezione dei dati personali*, cit., art. 29, 652-664 (commento di MANGIA); MELCHIONNA, *I principi generali*, cit., 59-63. I compiti del responsabile vanno analiticamente specificati da parte del titolare (art. 29, co. 4). Ne deriva che i responsabili possono essere tanto persone fisiche che persone giuridiche, pubbliche amministrazioni, enti, associazioni ed organismi, nominati dal titolare e preposti al trattamento di dati personali. Il termine «preposto» va interpretato nel senso che a tale soggetto è delegato dal titolare un autonomo potere decisionale e direttivo nell'ambito di compiti che gli sono stati specificatamente affidati.

[33] GARRI, *I soggetti che effettuano il trattamento: il titolare, il responsabile e l'incaricato*, cit., 148.

rizzare i soggetti (non medici) incaricati di trattare dati idonei a rivelare lo stato di salute e renderli noti all'interessato, così come previsto dall'art. 84, co. 2, Codice Privacy[34].

Si ricorda, poi, come si sia affermata nella pratica la tendenza ad affidare la prestazione di attività, sia primarie che collaterali, a soggetti esterni all'organizzazione imprenditoriale o alla pubblica amministrazione di riferimento (il c.d. *outsourcing*). Così, per esempio, si delega all'esterno la gestione di servizi elettronici o della sicurezza informatica. Non esistono limiti alla esternalizzazione delle attività e dei servizi nei confronti di soggetti terzi, non direttamente parte dell'azienda. La nomina di questi a responsabili del trattamento, funzionale ad un più agevole svolgimento dei rapporti, deve, però, essere espressa[35].

Per la preposizione del responsabile non è prevista alcuna forma tipica, anche se quella scritta risulta essere comunque preferibile in quanto la designazione non può mai essere implicita[36]. Ove il titolare del trattamento sia un soggetto pubblico, essa, deve invece necessariamente rivestire la forma scritta, in quanto dovranno esser applicate le

[34] *Ibidem*.

[35] In tali ipotesi deve essere chiarito il ruolo assunto dai soggetti (estranei all'organizzazione del titolare) ai quali viene affidata una determinata attività ai sensi della disciplina in materia di protezione dei dati personali. Questi possono, infatti, essere considerati collaboratori esterni del titolare allorquando coadiuvino quest'ultimo trattando dati personali anche al di fuori della relativa struttura, ma pur sempre nell'ambito di un'attività che ricade nella sfera di titolarità e di responsabilità di tale titolare: in questo caso costituiscono parte sostanziale del primo titolare e, quindi, vengono generalmente preposti a responsabili del trattamento; in via alternativa possono essere inquadrati come figure soggettive del tutto distinte dal titolare, in grado di decidere autonomamente in ordine al trattamento dei dati personali: tuttavia, in tal caso, essi sono da considerarsi autonomi titolari (v. Garante Privacy, *Parere*, 16 giugno 1999, in *Boll.*, 1999, n. 9, 19).

[36] Cfr. GARRI, *I soggetti che effettuano il trattamento: il titolare, il responsabile e l'incaricato*, cit., 151-153; DI COCCO, *Soggetti che effettuano il trattamento (Parte I - Titolo IV)*, cit., 130-131.

disposizioni in merito alle procedure, alle forme ed alle modalità per la delega di funzioni[37].

Il responsabile, quindi, viene preposto dal titolare del trattamento e da questi riceve istruzioni dettagliate con riferimento ai compiti a lui affidati. Il rapporto tra titolare e responsabile si articola in due fasi. Una prima fase costitutiva riguarda il momento della scelta del soggetto da designare come responsabile. Questa decisione rientra nella discrezionalità del titolare. Ove, però, la delega preveda anche lo svolgimento di alcune attribuzioni essa risulta sicuramente vincolata ad altri criteri quali la necessaria esperienza, capacità ed affidabilità di cui deve essere dotato il soggetto designando[38]. Una seconda fase riguarda, invece, l'obbligo di vigilanza da parte del titolare sull'attività del responsabile. Ciò con specifico riferimento alle direttive impartite. L'ultimo comma dell'art. 29 infatti recita:

> il responsabile effettua il trattamento attenendosi alle istruzioni impartite dal titolare, il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui al comma 2 e delle proprie istruzioni.

Ovviamente tali obblighi di vigilanza e controllo sono anche funzionali all'individuazione delle possibili responsabilità con riferimento al trattamento dei dati[39].

---

[37] Cfr. GARRI, *I soggetti che effettuano il trattamento: il titolare, il responsabile e l'incaricato*, cit., 152; BIANCA, BUSNELLI (a cura di), *La protezione dei dati personali*, cit., art. 29, 663-664.

[38] V. art. 29 Codice Privacy.

[39] Cfr. GARRI, *I soggetti che effettuano il trattamento: il titolare, il responsabile e l'incaricato*, cit., 153-157; DI COCCO, *Soggetti che effettuano il trattamento (Parte I - Titolo IV)*, cit., 132. L'art. 15 del Codice Privacy trattando dei possibili danni cagionati dal trattamento dei dati personali richiama l'art. 2050 del Codice Civile (esercizio di attività pericolose), stabilendo una responsabilità che prescinde dal grado di colpa ed è esclusa solo nel caso in cui si riesca a fornire la difficile prova di «aver adottato tutte le misure idonee ad evitare il danno». Appare, quindi, chiaro come l'attività di vigilanza

2.5.2 Titolarità del trattamento e Fascicolo Sanitario Elettronico

Lo scenario del trattamento dei dati sanitari in contesti digitalizzati si delinea sempre di più come un problema di gestione di flussi di dati e di *network*. Le informazioni, infatti, vengono scambiate stabilmente e secondo finalità comuni all'interno di organizzazioni complesse composte da una molteplicità di enti.

La funzione del titolare è ovviamente centrale nell'ambito di un FSE. Il Garante suggerisce che la titolarità del trattamento dei dati personali tramite FSE sia riconosciuta alla struttura o organismo sanitario nel suo complesso presso cui sono state redatte le informazioni sanitarie (ad es. l'azienda sanitaria o l'ospedale)[40]. Al titolare spetta il compito di organizzare l'intero processo di trattamento. Proprio per questo, egli risulta essere il principale destinatario degli obblighi di responsabilità e delle sanzioni previste dalla normativa sul trattamento dei dati personali. Le integrazioni introdotte dalla nuova formulazione dell'art. 4 si pongono su due piani: da un lato riguardano l'inciso relativo alla possibilità di prendere le decisioni relative agli elementi fondamentali del trattamento «anche unitamente ad altro titolare»: la c.d. co-titolarità si realizza, come abbiamo visto, nel caso in cui le scelte in tali ambiti siano riferibili a più soggetti; dall'altro, viene precisato che sono di competenza del titolare anche le decisioni in merito agli strumenti utilizzati per il trattamento.

Nel Documento di lavoro CCE Gruppo art. 29, a cui sopra si è già fatto riferimento, si ipotizzano diverse modalità di conservazione e di gestione dei dati in un sistema di c.d. «cartella clinica elettronica», ovvero il nostro FSE:

---

sull'operato del responsabile risponda al criterio della prova liberatoria della responsabilità civile. Per approfondimenti sul punto v., in prima battuta, F. GRITTI, *La responsabilità civile nel trattamento dei dati personali*, in CUFFARO, D'ORAZIO, RICCIUTO (a cura di), *Il codice del trattamento dei dati personali*, cit., 107-162.

[40] LG FSE, p. 4.3.

- c.d. «stoccaggio decentralizzato»: i fascicoli medici sono conservati dagli operatori sanitari, i quali hanno l'obbligo di registrare le informazioni sulle cure dei pazienti (all'interno di questa complessa struttura potrebbe rendersi necessaria l'individuazione di un organo centrale incaricato di gestire e controllare l'insieme del sistema e di garantirne la compatibilità con la protezione dei dati);
- c.d. «stoccaggio centralizzato»: il personale sanitario trasferisce la documentazione ad un sistema centrale di CCE (questo sistema garantisce una maggiore sicurezza tecnica e disponibilità: avremmo, infatti, un solo responsabile per tutto il sistema);
- controllo diretto del paziente: si consente al paziente di gestire le proprie cartelle mediche, fornendogli la possibilità di archiviare i dati inerenti la propria salute nell'ambito di uno speciale servizio *on-line* posto direttamente sotto il suo controllo – come accade in Francia (soluzione migliore in termini di autodeterminazione, ma che presenta problemi relativi all'esattezza ed alla completezza della documentazione, a meno che non si preveda la possibilità di un intervento correttivo del personale medico).

L'assetto tradizionale della gestione del FSE dei pazienti non è generalmente caratterizzato dalla realizzazione di una banca dati comune. Ciascun ente rimane cioè titolare dei trattamenti che effettua, dalla raccolta all'elaborazione, pur comunicando una parte cospicua di questi dati ad altri titolari all'interno della rete. Ciascun ente è titolare autonomo del trattamento e su di esso gravano gli obblighi previsti dalla normativa vigente, soprattutto con riferimento alla predisposizione di idonee e complete informative sul trattamento stesso. Tutto ciò prefigura scenari applicativi difficilmente governabili se non si accetta l'idea che il paziente sia messo in condizione di gestire appieno il suo rapporto con il «consenso», esercitando in modo diretto il proprio diritto di autodeterminazione informativa nell'ambito del FSE attraverso

un'interfaccia che, da remoto, registra ed implementa in tempo reale le scelte operate dall'interessato[41].

Cercando di tirare le fila di quanto sopra descritto, appare, dunque, chiaro come la scelta delle LG FSE sia quella di riconoscere, correttamente, la titolarità del sistema FSE, inteso come infrastruttura che viene resa disponibile agli operatori sanitari ed ai pazienti-utenti, alla ASL, cui compete porre in essere decisioni con riferimento alla finalità (tra l'altro in questo caso stabilita per legge), alla modalità di trattamento e, soprattutto in ambito informatico, alla sicurezza dell'intera piattaforma.

I dubbi ed i problemi sorgono quando si considera la gestione dei dati che nell'ambito del FSE vengono trattati. In questa prospettiva più soggetti (la ASL e le strutture private convenzionate nelle persone dei propri incaricati, gli MMG, i PLS, ecc.) di fatto trattano dati che essi condividono all'interno della struttura informatica, ma per i quali assumono, ciascuno con riferimento alla propria posizione, variegate posizioni di responsabilità. Per tale motivo si è evocato il concetto della co-titolarità, in quanto esso fotografa più precisamente ciò che in realtà avviene all'interno di un sistema che finisce per far perno sulla ASL[42].

[41] Diversamente, l'ipotesi riguardante la scelta di individuare un unico responsabile designato per gestire il FSE da parte dei vari titolari coinvolti è una soluzione che, pur rappresentando una semplificazione sul versante dell'accesso ai dati ed al sistema da parte del paziente-interessato al trattamento, presenta notevoli criticità dal punto di vista dell'effettività del rapporto fiduciario che la legge presuppone intercorrere tra il singolo responsabile e tutti i co-titolari del sistema FSE. Questi ultimi dovrebbero probabilmente provvedere ad una nomina per così dire standardizzata, svuotando di conseguenza di contenuti la disciplina prevista dal Codice Privacy.

[42] Come primi spunti ricostruttivi della reale portata prescrittiva di tale concetto giuridico v. quanto riportato *supra* in nt. 30. Anche su questo aspetto si avverte come necessario un intervento diretto del legislatore che vada a declinarne il significato nel contesto dell'intero fenomeno di FSE.

2.6 Affidamento con riferimento ai dati inseriti nel Fascicolo Sanitario Elettronico

È necessario concepire un meccanismo che permetta di ricostruire le «situazioni di responsabilità» rispetto alla generazione di ciascun singolo dato reso disponibile nel FSE (si allude evidentemente ad un sistema di tracciamento tramite file di *log* e di validazione dei documenti attraverso firme elettroniche[43]). Occorre rilevare come un sistema di *audit*, in grado di tracciare l'attività degli utenti, permettendo di stabilire *ex post* eventuali responsabilità, rappresenti un elemento imprescindibile in un sistema di FSE. Non sembra azzardato affermare che, in questo caso, la tecnologia offra la possibilità di interpretare le esigenze di tutela con un livello di effettività impensabile nell'epoca predigitale[44]. Non solo la generazione di un singolo dato dovrebbe venir

[43] La disciplina delle firme elettroniche nell'ordinamento italiano si ritrova nel già citato CAD, il quale è stato, come visto, sul punto recentemente modificato dal d.lgs. 235/2010. Per approfondimenti, che evidentemente si riferiscono alla disciplina precedente alla novella, v. PASCUZZI, *Il diritto dell'era digitale*, cit., 95-122, ivi riferimenti.

[44] Il valore probatorio dei file di *log* è oggetto di discussione, data la possibile modificabilità degli stessi. Il Trib. di Chieti si è occupato della loro rilevanza nel processo penale affermando che: «le attività di apprensione dei file di *log* da parte della polizia giudiziaria devono essere accompagnate da un attento controllo circa le modalità di conservazione dei dati informatici, allo scopo di verificare l'assenza di manipolazioni e la conseguente genuinità delle evidenze digitali; in mancanza di tali inadempimenti, i file di *log*, specie ove provengano dalla stessa persona offesa, costituiscono materiale del tutto insufficiente a fondare qualsivoglia affermazione di responsabilità al di là del ragionevole dubbio»: v. F. CAJANI, *Alla ricerca del log (perduto)*. Nota a Trib. Chieti, sez. pen., 30 maggio 2006, n. 139, in *Diritto dell'Internet*, 2006, 573. Il problema rinvia alla c.d. *computer forensics*: sul punto v. PASCUZZI, *Il diritto dell'era digitale*, cit., 256-259; G. FAGGIOLI, A. GHIRARDINI, *Computer forensics: il panorama giuridico italiano*, in *Ciberspazio e dir.*, 2007, fasc. 3, 329; G.B. GALLUS, *Verifiche sull'accesso ad Internet dei dipendenti e controlli preventivi*. Nota a ord. Trib. Perugia 20 febbraio 2006, in *Dir. informazione e informatica*, 2007, 200; L. LUPARIA, G. ZICCARDI, *Investigazione penale e tecnologia informatica, L'accertamento del reato tra progresso scientifico e garanzie fondamentali*, Milano 2007. Cfr. anche M. COLONNELLO, *La prova informati-*

tracciata e validata, ma anche la sua semplice visualizzazione ed il singolo accesso. Non è precluso ipotizzare un sistema che sappia generare un messaggio di avvertimento (ad esempio tramite *e-mail*) diretto a rendere edotto il paziente circa il fatto che un dato sanitario che lo riguarda (in regime di associazione con i dati personali del paziente) è stato visualizzato, consentendo di identificare il soggetto che ha avuto accesso ai suoi dati mediante un codice, anche in previsione di un'azione tesa a verificare che i propri diritti non siano stati violati. Certo, un accorgimento di tal fatta rischierebbe di generare un'eccessiva ridondanza (allertando il paziente talvolta senza motivo e fomentando inutili controversie). Nondimeno, un modello che cercasse di incorporare, anche in maniera flessibile e modulabile, questo tipo di impostazione consegnerebbe all'interessato un formidabile strumento di controllo atto a verificare che i dati che lo riguardano siano sempre trattati nel rispetto delle condizioni di legittimità previste dalla legge.

Un controllo di questo genere, sebbene non necessariamente alternativo alla definizione preventiva dei livelli di accesso, appare essere più funzionale e di più semplice attuazione pratica. Le informazioni relative agli accessi servirebbero al paziente a verificare, quando lo volesse, il motivo della visualizzazione dei suoi dati, nonché di chiedere al titolare spiegazioni a tal riguardo (dando effettività alle prerogative di cui all'art. 7 Codice Privacy)[45].

---

ca nel processo civile, 2009, in Rete: <http://www.jei.it/approfondimentigiuridici/notizia.php?ID_articoli=592>.

[45] A tal proposito le LG FSE, p. 6.4 così dispongono: «All'interessato deve essere fornito senza ritardo un riscontro compiuto e analitico in merito alle sue eventuali istanze (artt. 7, 8, 9, 10 e 146 del Codice). In particolare, deve essere fornito riscontro alle richieste di accesso ai dati personali estrapolando le informazioni oggetto dell'accesso e comunicandole all'interessato con modalità tali da renderne agevole la comprensione, se del caso trasponendole su supporto cartaceo o informatico; a tali istanze può essere opposto un rifiuto nei soli casi previsti dal Codice (art. 8)». Sebbene una disposizione di tal sorta possa rappresentare nel breve periodo un problema da un punto di vista gestionale-organizzativo per il titolare del trattamento a cui questa richiesta venisse posta, non si può non sottolineare la sua opportunità in vista di una piattaforma di FSE real-

Un punto sicuramente problematico si profila nell'implementare un modello di FSE che faccia propri anche i dati prodotti direttamente dal cittadino-paziente. Esso concerne il livello di affidamento che gli attori professionali del sistema, MMG, PLS, ma anche gli operatori incaricati della ASL, riporranno su di essi. Non è peregrino obiettare, a tal riguardo, che il personale medico, tendenzialmente, non sia predisposto a confidare su un'informazione, magari imprecisa o non veritiera, generata direttamente dal paziente, temendo di essere indotto in errore; ovvero potrebbe preoccuparsi di essere accusato di aver sbagliato, ove decida di non prendere in considerazione questa informazione ed essa si dimostri veritiera.

Questi timori possono essere gestiti considerando l'opportunità di implementare i seguenti accorgimenti nell'allestire un sistema di FSE.

In primis, il sistema dovrebbe essere concepito in modo da lasciare sempre traccia dell'identità del soggetto che ha inserito le informazioni e del momento preciso in cui ciò è avvenuto. La struttura informativa dovrebbe, poi, garantire l'inalterabilità del dato prodotto dal cittadino: si potrà prevedere che il paziente possa modificare i dati, magari immessi per errore, ma di questo la struttura informatica dovrà essere in grado di tenere traccia, prevedendo sempre una sorta di «storico» delle *entry* dell'utente.

MMG e PLS potranno, pertanto, gradualmente attribuire a questo tipo di informazioni auto-prodotte dal paziente un livello di fiducia corrispondente a quello che sussiste anche nel contesto «reale» di un qualsiasi percorso di cura che avviene *vis-à-vis*. Lo scenario digitale non è diverso e non può essere dissociato dalle dinamiche di fiducia che prendono corpo nel mondo «fisico».

---

mente in grado di garantire i diritti dei singoli con riferimento al controllo sul trattamento dei propri dati sanitari.

Se oggi, infatti, un medico incontrasse per la prima volta un paziente e fosse da costui investito da una montagna di «carte» attestanti una serie di informazioni relative alla propria storia clinica pregressa (analisi, annotazioni personali, ricette di farmaci assunti, ecc.), è verosimile attendersi che egli non sarebbe portato a riporre su tali informazioni un particolare grado di fiducia. Ne conseguirebbe la legittima richiesta di nuove analisi, nuove indagini, ecc., finché il medico, convintosi della veridicità ed accuratezza del quadro diagnostico, non proponga al paziente il programma terapeutico ritenuto opportuno in scienza e coscienza. Molto diverso è, invece, il contesto della fiducia fra un MMG e un paziente in acuzie o cronico che – si ipotizzi – si reca due volte alla settimana presso lo studio del suo MMG, effettuando quotidiane automisurazioni, e le sottoponga al curante. Questo tipo di interazione sviluppa un rapporto di fiducia tale da potersi facilmente trasporre anche in quella garantita dalla struttura informatica, che, in più, permetterebbe una gestione sicuramente più efficiente ed efficace dell'intero percorso curativo[46].

2.6.1 Il rapporto fiduciario tra medico e paziente

Un aspetto critico del sistema FSE, e della sanità elettronica in generale, è rappresentato dal rischio che questa innovazione inneschi un processo di disumanizzazione della relazione medico-paziente[47].

[46] Si v. le «Linee Guida in materia di trattamento di dati personali e sanitari nell'ambito del sistema Cartella Clinica del Cittadino (TreC)», cit.

[47] Più in generale è vivo un dibattito sulla c.d. umanizzazione degli ospedali e delle cure: il rapporto tra medico e paziente è anche un rapporto di rispetto verso la debolezza e la sofferenza. Per approfondimenti v. A. BRUSCO, *Il mondo della salute. Le sfide dell'umanizzazione*, 2003, in Rete: <http://www.sentieriformativi.it/articolo.asp?id=2#_ftnref16>; J. HOWARDS, A. STRAUSS, *Humanizing Health Care,* New York, 1997; E. SGRECCIA, *Non archiviare l'impegno per l'umanizzazione della medicina,* in *Medicina e Morale*, 1986, fasc. 2, 267-270; A. BRUSCO, *Umanità per gli ospedali,* Bresso di Bedero, 1983; I. ILLICH, *Nemesi medica. L'espropriazione della salute,* Milano, 1977.

Questo rapporto umano si è costruito nei secoli secondo una struttura ritualizzata, che si estrinseca in una serie di comportamenti ove medico e paziente interagiscono secondo uno schema sociale che li porta a condividere conoscenze, problemi e preoccupazioni[48]. Il paziente, nel mondo reale, si reca fisicamente al cospetto del suo curante per esternare la propria sintomatologia, alla ricerca di una cura per i mali che lo affliggono. Il medico riceve questo «sfogo» e, alla luce delle informazioni raccolte e delle conoscenze di cui è depositario, elabora il corretto processo di diagnosi e di cura, secondo una dinamica antica quanto la medicina.

Oggi nella relazione tra il medico ed il paziente si inserisce la tecnologia informatica. Il rapporto viene mediato dallo strumento digitale anche se i soggetti continuano ad interagire fisicamente. La visita sarà preceduta dall'apertura del fascicolo sanitario che riguarda il paziente, in modo tale da mettere il professionista nella situazione di comprendere, grazie ad un rapido aggiornamento, la storia clinica del suo assistito. L'interazione mediata anche dalla tecnologia arricchisce questo quadro. Da sempre il medico consulta le proprie cartelle per verificare il tipo e la qualità di informazioni di cui già dispone. Con la sanità elettronica, egli utilizza un aggregatore di dati immensamente più rapido e potente di qualsiasi ordine precostituito attraverso la raccolta e la giustapposizione di informazioni veicolati da un supporto cartaceo.

Se, invece, il rapporto avviene a distanza il rischio di «disumanizzazione» potrebbe apparire più fondato. Anche qui si tratta di un problema «culturale». Tralasciando le nuove generazioni[49], le quali po-

[48] Per approfondimento v. B.J. GOOD, *Medicine, Rationality and Experience: An Anthropological Perspective*, Cambridge, 1994. V. anche GHERARDI, STRATI, *La telemedicina*, cit., 68 ss.; sul rapporto medico paziente troviamo pure interessanti considerazioni in chiusura del saggio SINHA, *An Overview of Telemedicine*, cit.; e in RICCIO, *Privacy e dati sanitari*, cit., 249-252.

[49] Ci si riferisce ai c.d. «nativi digitali»: v. M. PRENSKY, *Digital Natives, Digital Immigrants*, in *On the Horizon*, vol. 9, n. 5, ottobre 2001. Si rimanda agli approfondimenti che verranno svolti nel paragrafo del prossimo capitolo dedicato alla delega

trebbero addirittura sentirsi maggiormente a loro agio utilizzando un'infrastruttura tecnologica che ormai appartiene alla propria esperienza quotidiana (si pensi all'incredibile diffusione dei *social network*, ed in generale di piattaforme che veicolano le comunicazioni degli utenti secondo canali sempre nuovi), anche nel caso dei c.d. «immigrati digitali» (cioè i nati prima degli anni novanta), il problema appare meno grave di quel che può sembrare. La fiducia tra medico e paziente si costruisce sulla base di un reciproco scambio di informazioni, cui fa da sfondo un'effettiva conoscenza tra i due soggetti, a prescindere dal *medium* utilizzato, sia che si tratti, o non, di documentazione cartacea o di trasmissioni di file *on-line*.

La questione è di nuovo «culturale»: occorre, e occorrerà sempre più in futuro, che all'implementazione di piattaforme tipo FSE corrisponda un'adeguata alfabetizzazione informatica, sia per gli operatori che per gli utenti. I danni maggiori si verificano, infatti, quando non si ha adeguata conoscenza dello strumento che si utilizza. Un'efficace opera di informazione (agli utenti) e di formazione (ai prestatori di servizi destinati ad impiegare il nuovo strumento) servirà ad agevolare nuove forme di collaborazione rispetto a quelle derivanti da relazioni umane (fisiche) molto spesso soggette a schemi comportamentali cristallizzati dalle abitudini.

2.7 Accesso modulare al Fascicolo Sanitario Elettronico

L'accesso al FSE dovrebbe essere concesso all'operatore sanitario qualora costui abbia materialmente redatto la documentazione sanitaria relativa al paziente di cui si è assunto la cura, sempre che quest'ultimo lo abbia consentito nei termini sopra indicati[50]. In riferi-

all'accesso da parte del paziente-interessato ai servizi offerti dal FSE ed alle considerazioni di carattere generale sul c.d. *digital divide* generazionale.

[50] LG FSE, p. 5 «Accesso ai dati personali contenuti nel Fascicolo sanitario elettronico e nel *Dossier* sanitario».

mento a ciò va sottolineato anche l'aspetto della temporalità: l'accesso al FSE dovrebbe essere circoscritto al periodo di tempo indispensabile per espletare le operazioni di cura per le quali è abilitato il soggetto che accede. Ad esempio, se il paziente si dovesse recare nel pronto soccorso di un'altra azienda sanitaria o, addirittura, di un'altra regione, la visualizzazione dei dati sanitari che lo riguardano contenuti nel FSE dovrebbe essere limitata al periodo in cui egli risulta ospedalizzato.

Si presenta, allora, l'esigenza di concepire una «organizzazione modulare» della struttura del FSE volta a limitare l'accesso dei diversi soggetti abilitati alle sole informazioni a loro indispensabili e solo per il tempo in cui questo accesso è legittimo (principio di necessità). L'accesso ai dati dovrebbe essere garantito con riferimento alle sole informazioni correlate con la patologia in cura[51].

Si rileva come in alcune esperienze straniere (v. quella francese), l'accesso ai dati sanitari contenuti nel FSE sia gestito in base alle diverse specialità di ciascun medico. Ciò è avvenuto anche in alcune sperimentazioni a livello nazionale[52]. Così, ad esempio, un medico specializzato in ortopedia dovrebbe essere in grado di visualizzare solo i dati che si riferiscono alla sua specialità e non quelli concernenti le visite dermatologiche. Questa soluzione, che richiede, comunque, un impegno diretto da parte dei professionisti sanitari nello stabilire le diverse categorie mediante le quali catalogare e trattare i dati, appare difficoltosa in quanto risulta arduo determinare *ex ante* il livello di pertinenza di ogni singolo dato sanitario, soprattutto nei casi di specialità mediche che condividono simili sintomatologie. Inoltre, questo approccio appare

[51] Determinate categorie di soggetti, quali ad esempio quella dei farmacisti, dovrebbero avere un accesso ancor più limitato ai soli dati indispensabili all'erogazione ad esempio di prodotti farmaceutici.

[52] LG FSE, p. 5.3, 5.4, 5.5.

poco sensato a fronte delle critiche sempre più spesso rivolte a mettere in evidenza l'eccessiva frammentazione della medicina occidentale[53].

La soluzione va, piuttosto, ricercata nel corretto bilanciamento tra l'esigenza di garantire al paziente-interessato una reale realizzazione del principio di autodeterminazione, anche con riferimento ai livelli di accesso nei confronti delle informazioni sanitarie che lo riguardano, e le imprescindibili esigenze di cura e prevenzione proprie del SSN e degli operatori sanitari. Se allora sarà corretto limitare attentamente l'accesso ai dati sanitari contenuti nel FSE da un punto di vista della gerarchia verticale (medici, infermieri, amministrativi), non lo sarà, se non nei casi più evidenti o in presenza di informazioni particolarmente riservate, con riferimento alle diverse specialità mediche[54].

---

[53] Dagli anni cinquanta la medicina si è andata caratterizzando per un'eccessiva esaltazione delle specializzazioni e per una progressiva frammentazione delle conoscenze e competenze sub-specialistiche, dovute anche allo straordinario sviluppo della tecnologia diagnostica strumentale e di farmaci innovativi; tutto ciò ha determinato uno spostamento di interesse dalla persona alle malattie di un organo o di un apparato. Questa frammentazione delle specialità cliniche fa perdere la visione d'insieme della persona e della salute e determina un rapporto perverso tra servizio offerto e cura del paziente: all'offerta di servizi tecnologicamente via via più avanzati corrispondono spesso relazioni umane sempre più ridotte e distaccate. Cfr. A. PAGNI, *Dalla condotta medica alla medicina telematica*, Lettura magistrale alle Giornate nazionali di studio in medicina telematica, 8-9-10 aprile 2010, Firenze, in Rete: <http://www.ordinemedicilatina.it/system/files/DALLA+CONDOTTA+MEDICA+ALLA+MEDICINA+TELEMATICA.pdf>.

[54] Le LG FSE al pp. 5.6 e 5.7 assicurano una tutela rafforzata per una particolare categoria di informazioni. Nel testo viene, così, fatto esplicito riferimento alle disposizioni normative a tutela dell'anonimato della persona tra cui quelle a tutela delle vittime di atti di violenza sessuale o di pedofilia (l. 15 febbraio 1996, n. 66; l. 3 agosto 1998, n. 269 e l. 6 febbraio 2006, n. 38), delle persone sieropositive (l. 5 giugno 1990, n. 135), di chi fa uso di sostanze stupefacenti, di sostanze psicotrope e di alcool (d.P.R. 9 ottobre 1990, n. 309), delle donne che si sottopongono a un intervento di interruzione volontaria della gravidanza o che decidono di partorire in anonimato (l. 22 maggio 1978, n. 194; d.m. 16 luglio 2001, n. 349), nonché con riferimento ai servizi offerti dai consultori familiari (l. 29 luglio 1975, n. 405). Il titolare del trattamento può, in tali casi, decidere di non inserire tali informazioni nel FSE, ovvero di inserirle a fronte di una specifica manifestazione di volontà dell'interessato, il quale potrebbe anche legittima-

2.8 Comunicazione dei dati all'interessato ed art. 84 Codice Privacy

Per quanto riguarda i flussi in uscita da un sistema di FSE, molte esperienze regionali italiane hanno già riconosciuto al paziente la possibilità di accedere ad alcuni dati nei propri sistemi informativi (per ora limitatamente ai referti) tramite servizi telematici a tal scopo predisposti[55].

La messa in opera di piattaforme di questo tipo presenta, tuttavia, molteplici criticità sul versante della protezione dei dati personali. Il Garante, nel corso della relazione annuale del 9 febbraio 2005 in materia di consegna dei referti medici, dopo aver trattato dei casi di numerose ASL che li trasmettevano tramite fax di altri soggetti (tabaccherie, uffici privati, ecc.), ricordava come il Codice Privacy preveda, invece, che i dati personali inerenti lo stato di salute possano essere resi noti al paziente solo per il tramite del medico designato dallo stesso, ai sensi dell'art. 84 (norma piuttosto negletta nelle trattazioni dottrinali correnti, di cui oltre cercheremo di fornire un'analisi più approfondita)[56].

---

mente richiedere che tali informazioni siano consultabili solo da parte di alcuni soggetti dallo stesso individuati (ad es. specialista presso cui è in cura).

[55] V. oltre l'approfondimento in tema di refertazione *on-line*.

[56] Il Codice stabilisce, inoltre, che il personale infermieristico e di assistenza sanitaria possa venire a conoscenza delle informazioni sullo stato di salute dei pazienti, solo per quanto riguarda quelle strettamente necessarie per il migliore svolgimento delle loro funzioni, e di trattarle comunque in conformità alla normativa in materia di protezione dei dati personali, v. la prescrizione del Garante del 9 novembre 2005 (in *Boll*., n. 65/novembre, 2005, 0) in cui si afferma che «Gli esercenti le professioni sanitarie e gli organismi sanitari possono comunicare all'interessato informazioni sul suo stato di salute solo per il tramite di un medico (individuato dallo stesso interessato, oppure dal titolare del trattamento) o di un altro esercente le professioni sanitarie che, nello svolgimento dei propri compiti, intrattenga rapporti diretti con il paziente (ad es., un infermiere designato quale incaricato del trattamento ed autorizzato per iscritto dal titolare). […] Il personale designato deve essere istruito debitamente anche in ordine alle modalità di consegna a terzi dei documenti contenenti dati idonei a rivelare lo stato di salute dell'interessato (es. referti diagnostici). In riferimento alle numerose segnalazioni pervenute, va rilevato che le certificazioni rilasciate dai laboratori di analisi o dagli altri

L'accesso al FSE deve essere consentito al paziente-interessato nel rispetto delle cautele previste in tale articolo, il quale inserisce la previsione di un filtro nella comunicazione dei dati sanitari tra il paziente ed il dato stesso, rappresentato da un medico o da un esercente le professioni sanitarie[57]. Sul punto, le LG FSE e le LG Referti sono state piuttosto laconiche, evitando di fornire una reale linea di indirizzo atta ad implementare la *ratio* di questa previsione normativa. La tematica merita però un approfondimento, specie se si abbandona (o meglio: se si integra) la definizione di FSE che le LG prendono in considerazione per accendere l'attenzione anche sul profilo relativo al FSE aperto al paziente-utente del sistema.

Sul tema dell'accesso ai dati sanitari abbiamo già avuto modo di citare alcune fonti normative sia a livello comunitario che nazionale (tra tutte, vedi la Raccomandazione della Commissione del 2 luglio 2008 sull'interoperabilità transfrontaliera dei sistemi di cartelle cliniche elettroniche ed il documento rilasciato il 31 marzo 2005 «Una politica per la Sanità Elettronica» dal TSE).

Punto cardine dell'architettura deve essere il rispetto dell'autodeterminazione: la decisione del paziente sul come e quando utilizzare i dati che lo riguardano deve rivestire un ruolo di garanzia fondamentale[58]. Questo principio, che nella più ampia tematica del FSE comporta il controllo anche dell'accesso da parte degli operatori sanitari ai dati ine-

---

organismi sanitari possono essere ritirate anche da persone diverse dai diretti interessati, purché sulla base di una delega scritta e mediante la consegna delle stesse in busta chiusa».

[57] Per approfondimenti sull'art. 84 Codice Privacy, v. BIANCA, BUSNELLI (a cura di), *La protezione dei dati personali.* cit., art. 84, 1303 (commento di E. PALMERINI); G.M. RICCIO, *Privacy e dati sanitari*, in F. CARDARELLI, S. SICA, V. ZENO-ZENCOVICH (a cura di), *Il codice dei dati personali. Temi e problemi*, Milano, 2004, 298-300; CAGGIA, *Il trattamento dei dati sulla salute, con particolare riferimento all'ambito sanitario*, cit., 425-430; MONDUCCI, PASETTI, *Il trattamento dei dati sanitari e genetici (Parte II – Titolo V)*, cit., 273-274.

[58] V. Documento CCE art. 29, parte III «Riflessioni su un quadro giuridico adatto per i sistemi di CCE», primo paragrafo «Rispetto dell'autodeterminazione».

renti la salute del paziente e la conseguente necessaria modularità dei dati inseriti, obbliga a focalizzare l'attenzione anche sull'aspetto dell'informativa concernente il trattamento che così viene posto in essere.

Conviene iniziare l'analisi partendo dal dato positivo accolto nel nostro ordinamento. L'art. 84 Codice Privacy – rubricato «Comunicazione dei dati all'interessato» – così recita:

> 1. I dati personali idonei a rivelare lo stato di salute possono essere resi noti all'interessato o ai soggetti di cui all'articolo 82, comma 2, lettera a), da parte di esercenti le professioni sanitarie ed organismi sanitari, solo per il tramite di un medico designato dall'interessato o dal titolare. Il presente comma non si applica in riferimento ai dati personali forniti in precedenza dal medesimo interessato. 2. Il titolare o il responsabile possono autorizzare per iscritto esercenti le professioni sanitarie diversi dai medici, che nell'esercizio dei propri compiti intrattengono rapporti diretti con i pazienti e sono incaricati di trattare dati personali idonei a rivelare lo stato di salute, a rendere noti i medesimi dati all'interessato o ai soggetti di cui all'articolo 82, comma 2, lettera a). L'atto di incarico individua appropriate modalità e cautele rapportate al contesto nel quale è effettuato il trattamento di dati.

Vengono così ribaditi i principi già espressi dall'art. 23, co. 2, della precedente l. 675/1996[59]. Le novità riguardano l'indicazione dei soggetti per conto dei quali la comunicazione è effettuata («da parte di esercenti le professioni sanitarie ed organismi sanitari»), con cui si chiarisce il contesto di applicazione della norma, circoscrivendola soltanto a quello sanitario, nonché l'inciso finale, che conferma la non applicabilità della regola ai dati personali forniti precedentemente dal paziente. Un'altra sicura innovazione è rappresentata dal secondo comma dell'art. 84 Codice Privacy, il quale consente anche ai professionisti sa-

[59] Art. 23, co. 2, l. 675/1997: «I dati personali idonei a rivelare lo stato di salute possono essere resi noti all'interessato […] solo per il tramite di un medico designato dall'interessato o dal titolare».

nitari diversi dai medici di svolgere la funzione disciplinata in virtù di un atto di incarico all'uopo ricevuto[60].

Viene inserito, quindi, un intermediario tra i dati e l'interessato al fine di rispondere, da un lato, all'esigenza di agevolare la comprensione dei dati clinici da parte del paziente, dall'altro, a quella di filtrare l'informazione ottenuta al fine di ritrasmetterla successivamente in una forma rispettosa dei principi che regolano la relazione terapeutica tra medico e paziente stesso.

Sul piano ricostruttivo, la regola dell'intermediazione di un soggetto professionista medico trova un suo primo antecedente in disposizioni sovranazionali, ed in particolare nella Raccomandazione n. R (89) 2 del Consiglio d'Europa, ove si prospettava, agli Stati membri la possibilità di prevedere tale comunicazione mediata in ragione della delicatezza e della possibile complessità del contenuto, nonché del grave pregiudizio che dalla conoscenza distorta dell'informazione può derivare. La formulazione di tale indicazione è stata però criticata da parte di alcuni commentatori, i quali hanno evidenziato il carattere di privilegio in favore della professione medica che la regola presenta, la quale sembrerebbe istituire una sorta di controllo sulla circolazione dei dati sanitari[61]. Di fronte al grado di cultura media del cittadino, questa previsione può apparire frutto di un'eccessiva cautela nei confronti dell'utente, se non (più esplicitamente) di un esagerato paternalismo.

In realtà, l'intermediazione dell'operatore qualificato nella comunicazione dei dati all'interessato trova conferme – sempre a livello sovranazionale – in altri documenti, non dotati di forza vincolante, ma

[60] Cfr. CAGGIA, *Il trattamento dei dati sulla salute, con particolare riferimento all'ambito sanitario*, cit., 426-427; F. MASCHIO, *Il trattamento dei dati sanitari. Regole generali e particolari trattamenti per finalità di rilevante interesse pubblico*, in SANTANIELLO (a cura di), *La protezione dei dati personali*, cit., 498-499.

[61] Cfr. CAGGIA, *Il trattamento dei dati sulla salute, con particolare riferimento all'ambito sanitario*, cit., 427; V. ZAMBRANO, *Dati sanitari e tutela della sfera privata*, in *Dir. informazione e informatica*, 1999, 1, 19; CIATTI, *La protezione dei dati idonei a rivelare lo stato di salute nella l. 675 del '96,* cit., 391.

pur sempre conformanti l'attività dei legislatori nazionali. Ci riferiamo, ad esempio, al Considerando n. 42 della Direttiva 95/46/Ce[62]; alla Raccomandazione N.R. (81) 1 del Consiglio d'Europa del 23 gennaio 1981, la quale prevede al paragrafo 6.1 che tale filtro sia previsto per legge; alla Raccomandazione del 23 settembre 1980 dell'O.E.C.D. (Linee guida sulla protezione della vita privata e su i flussi transfrontalieri di dati di carattere personale). La regola prevista dall'art. 23, co. 2, della nostra legge 675/1996, poi trasposta nel nuovo articolo 84 Codice Privacy, è presente anche negli ordinamenti di altri Paesi europei[63].

[62] Il quale così recita: «gli stati membri possono a beneficio della persona interessata o a tutela dei diritti e della libertà altrui, limitare il diritto d'accesso e di informazione; che possono, ad esempio, precisare che l'accesso ai dati medici è possibile soltanto per il tramite del personale sanitario». Lo stesso art. 13 della Direttiva 95/46/Ce riconosce agli stati membri la possibilità di adottare disposizioni legislative intese a limitare la portata degli obblighi e dei diritti previsti, tra le altre, dalla disposizione dell'art. 12 (relativo al diritto d'accesso), qualora tale restrizione risulti essere una misura necessaria al fine di salvaguardare la protezione della persona interessata o dei diritti e delle libertà altrui.

[63] Di seguito alcuni esempi. Francia: *Loi* n. 78-17 *du* 6 *janvier* 1978 *relative à l'informatique, aux fichiers et aux libertés*, art. 43: «Lorsque l'exercice du droit d'accès s'applique à des données de santé à caractère personnel, celles-ci peuvent être communiquées à la personne concernée, selon son choix, directement ou par l'intermédiaire d'un médecin qu'elle désigne à cet effet, dans le respect des dispositions de l'article L. 1111-7 du code de la santé publique». L'art. 1111-7 del *Code de la santé publique* conferma al secondo comma che: «Elle [Toute personne] peut accéder à ces informations directement ou par l'intermédiaire d'un médecin qu'elle désigne et en obtenir communication, dans des conditions définies par voie réglementaire au plus tard dans les huit jours suivant sa demande et au plus tôt après qu' un délai de réflexion de quarante- huit heures aura été observé. Ce délai est porté à deux mois lorsque les informations médicales datent de plus de cinq ans ou lorsque la commission départementale des hospitalisations psychiatriques est saisie en application du quatrième alinéa». L'esperienza francese ci consegna quindi una regola che lascia al paziente la scelta della procedura per la comunicazione dei dati sanitari. Belgio: *Loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel*, 8 dicembre 1992, art. 10 § 2: «Sans préjudice de l'article 9, § 2, de la loi précitée, la communication peut être effectuée par l'intermédiaire d'un professionnel des soins de santé choisi par la personne concernée, à la demande du responsable du traitement ou de la personne concernée». Portogallo: *Lei da protecçao*

Tornando al nostro ordinamento, appare evidente come l'art. 84, letto in stretta connessione con gli artt. 1 e 2, co. 1, del Codice Privacy (i quali sanciscono l'esistenza di una situazione soggettiva nuova con riferimento al trattamento dei propri dati personali), attribuisca una particolare qualificazione all'obbligo di informazione scaturente dal rapporto di cura, riconoscendo in capo al medico una sorta di «privilegio terapeutico»[64]. In base a tale principio, il medico avrebbe la facoltà di non rivelare al paziente alcuni elementi della diagnosi o di carattere prognostico idonei a compromettere lo stesso scopo della cura (v. nello stesso senso anche la Convenzione bioetica sulla biomedicina – c.d. Convenzione di Oviedo – del 1997 del Consiglio d'Europa, il cui art. 10 riconosce sia il diritto del paziente di conoscere ogni informazione raccolta sulla sua salute, sia quello di non essere informato e stabilisce

de dados pessoais del 26 ottobre 1998, art. art. 11 § 5: «O direito de acesso à informação relativa a dados da saúde, incluindo os dados genéticos, é exercido por intermédio de médico escolhido pelo titular dos dados». Spagna: *Ley Orgánica* 15/1999, *de* 13 *de diciembre, de Protección de Datos de Carácter Personal*, art. 8 (*Datos relativos a la salud*): «Sin perjuicio de lo que se dispone en el artículo 11 respecto de la cesión, las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad», rimandando quindi alla legislazione speciale, statale e delle autonomie locali, in materia di trattamento di dati sanitari la relativa disciplina. Stessa regola in un Paese europeo ma extracomunitario come la Svizzera: Legge Federale del 19 giugno 1992 sulla protezione dei dati (LPD), art. 8 § 3: «Il detentore della collezione di dati può comunicare alla persona interessata dati concernenti la salute, per il tramite di un medico da essa designato».

[64] Sul più generale diritto a non sapere da parte del singolo, così si esprime un famoso autore: «si tratta di una nozione di identità che non corrisponde a quella classica, in cui il diritto di non sapere rappresenta uno dei fattori essenziali per la libera costruzione della personalità», in S. RODOTÀ, *Privacy e costruzione della sfera privata. Ipotesi e prospettive*, in *Politica del dir.*, 1991, 525, 534.

la possibilità di prevedere restrizioni ad entrambi questi diritti da parte della legge nazionale, purché nell'interesse del malato)[65].

Sul problema ha peraltro avuto modo di pronunciarsi in più occasioni lo stesso Garante, il quale, per i casi in cui si discuteva circa la volontà del paziente di conoscere le determinazioni espresse sul suo stato di salute da parte di medici consulenti di compagnie assicurative, ha sempre confermato la necessità che tale accesso avvenisse per il tramite di un medico scelto dall'interessato stesso o dal titolare[66].

Abbiamo descritto la *ratio* della previsione di un «filtro» nella comunicazione del dato sanitario al paziente. È, tuttavia, evidente come, partendo dalla prospettiva della costruzione di un'architettura che faccia dell'accesso ai dati sanitari da parte dell'utente-paziente la sua prima ragione d'essere, una previsione normativa che si muova in tale direzione incontri non pochi problemi applicativi, poiché introduce un ulteriore ostacolo all'ideazione di una piattaforma informatica idonea ad avvicinare il cittadino alla prestazione sanitaria, per rendere più efficace ed efficiente l'attività del servizio sanitario.

A voler dare un reale significato al requisito dell'intermediazione, bisogna ritenere che il medico non possa limitarsi a fungere da mero veicolo di trasmissione di un'informativa che riporti meccanicamente i dati. La *ratio* della disposizione vuole che al paziente sia fornita una spiegazione, che, seppur sintetica, sia profilata sulla descrizione delle condizioni psico-fisiche dell'interessato. Il diritto all'informazione medica è, quindi, soddisfatto solo se l'interessato è posto in grado di comprendere agevolmente il significato dei dati che lo riguardano.

---

[65] Cfr. BIANCA, BUSNELLI (a cura di), *La protezione dei dati personali*, cit., art. 84, 1310-1312.

[66] V. Provv. Garante Privacy del 2 maggio 2002, 20 marzo 2002, 19 e 27 febbraio 2002. Più in particolare si v. il Provv. Garante Privacy 9 febbraio 2005 sul rispetto della dignità nelle strutture sanitarie sopra ricordato. V. anche BIANCA, BUSNELLI (a cura di), *La protezione dei dati personali.* cit., art. 84, 1313-1314.

Tale requisito non sembra essere un ostacolo insuperabile per la trasposizione informatica della regola applicativa. Innanzitutto, la comunicazione tra il medico e l'interessato non deve necessariamente essere diretta, essendo già oggi nella facoltà di quest'ultimo delegare ad un amico o ad un parente il compito di conferire con il medico o di prendere visione delle proprie comunicazioni. In caso contrario, si profilerebbe un'irragionevole ingerenza nel potere di autogestione dei propri interessi che compete ad ogni individuo in possesso della capacità di agire. Questa osservazione permette di scartare l'ipotesi che la norma renda necessario prevedere, per esempio, un dispositivo informatico in grado di attestare che il medico sia *on-line* nello stesso momento in cui il paziente accede ai dati.

Ammettere, poi, che la comunicazione possa essere ritirata da terzi a ciò autorizzati, significa prevedere che l'intermediazione del medico possa avvenire per il tramite di un testo scritto che illustri il contenuto dei dati «grezzi». Se ciò vale per il supporto cartaceo, non si vede perché tale modalità applicativa non debba potersi applicare anche nel contesto di una comunicazione digitalizzata, che offre semmai maggiori garanzie in termini di integrità, affidabilità e confidenzialità.

Si potrà, allora, pensare ad una piattaforma che renda il dato sanitario accessibile all'utente-paziente solo quando al *record* sia stata allegata la comunicazione relativa all'interpretazione che dei dati sanitari il medico-filtro ha fornito.

Questa appare essere la soluzione proposta dal Garante Privacy nelle LG Referti laddove si legge:

> l'intermediazione potrebbe essere soddisfatta accompagnando la comunicazione del reperto con un giudizio scritto e la disponibilità del medico a fornire ulteriori indicazioni su richiesta dell'interessato[67].

[67] LG Referti, p. 5.2.

Tale passaggio delle LG potrebbe essere interpretato considerando il «referto» – il quale consiste appunto nella relazione scritta rilasciata dal medico sullo stato clinico del paziente – quale «giudizio scritto» del «reperto» – inteso come il risultato dell'esame clinico o strumentale, ad es. un'immagine radiografica[68]. Il tutto accompagnato dall'indicazione della possibilità di rivolgersi al medico al fine di ottenere ulteriori chiarimenti. Questa soluzione garantirebbe il superamento, in sede interpretativa, dell'altrimenti stringente locuzione «solo per il tramite» di cui all'art. 84 Codice Privacy.

Ad integrazione della soluzione testé prospettata, e venendo incontro alle ipotizzabili resistenze da parte del personale sanitario (in special modo degli MMG, che potrebbero rifiutare di essere investiti da questa mole di ulteriori compiti da svolgere), si può ipotizzare l'adozione di una struttura informativa che, non appena il paziente cerchi di accedere al dato di prima comunicazione, generi un avviso automatico (una sorta di *pop-up*), il quale renda edotto il paziente della necessità di recarsi dal proprio MMG per farsi esplicare i «dati grezzi» (esattamente come oggi accade quando si consegna all'interessato, come già visto sopra, una busta cartacea recante la dicitura «al medico curante», contenente gli esiti cartacei delle analisi di laboratorio cui il paziente si è sottoposto). Tale videata di *warning*, che potrebbe essere seguita da una successiva schermata di accettazione nella quale l'interessato dichiara di aver compreso l'avviso circa la necessità di ottenere dal proprio medico curante l'interpretazione del dato che lo riguarda, svolgerebbe una duplice finalità maieutica: da un lato, il paziente sarebbe informato del fatto che egli non è in grado di analizzare e capire il significato dei dati sanitari («grezzi») che lo riguardano; dall'altro incentiverebbe l'attività di esplicazione degli eventi clinici nei confronti dei pazienti, nella pra-

[68] *Ibidem*, p. 1.1.

tica purtroppo non sempre così accurata ed approfondita[69].

In seno al FSE i dati che necessitano di tale «filtro» andranno circoscritti, separandoli da quelli ai quali, invece, l'utente potrà accedere direttamente, perché a lui già noti (non dimentichiamo che la *ratio* della disposizione si esprime solo sul profilo del primo accesso cognitivo del paziente interessato al dato che lo riguarda) o perché da lui direttamente forniti (si pensi all'anamnesi raccolta dal curante e riportata nella FSE).

Esistono, poi, altre informazioni per le quali le idonee istruzioni alla lettura sono già state fornite, magari in corso di degenza o all'atto di dimissione: non appare sensato ritenere che il rilascio di copia, ad esempio della cartella clinica, anche se richiesto a distanza di tempo, debba soggiacere ad ulteriori ripetizioni. Occorrerà, quindi, predisporre all'uopo un sistema di tracciamento-identificazione di quei contenuti per i quali l'intermediazione è già avvenuta.

Si dovrà comunque considerare che il filtro di cui all'art. 84 Codice Privacy è destinato ad operare solo se il processo di comunicazione del dato fra produttore (ospedale, laboratorio di analisi) e fruitore finale (il paziente interessato) avvenga a distanza ed in modo impersonale (il caso più evidente è quello di un'analisi di laboratorio); mentre ciò non capita in caso di visita specialistica condotta sulla persona dell'interessato, laddove la prima diagnosi venga spiegata dal curante stesso al paziente interessato nel corso della visita.

L'analisi appena prospettata fa emergere un quadro caratterizzato sia da riferimenti normativi che di altra fonte, mancante però, da un certo punto di vista, di soluzioni pratiche che siano, al di là di ogni ragionevole dubbio, conformi alla disciplina in materia di trattamento dei dati personali. Il problema, però, è attuale e va risolto: enormi sono le potenzialità che i nuovi sistemi di sanità elettronica prospettano per

[69] Cfr. R.H. THALER, C.R. SUNSTEIN, *Nudge: Improving Decisions About Health, Wealth, and Happiness*, New Haven - London, 2008, *passim*.

poter nascondersi dietro la lacunosità e mancanza di chiarezza del dettato normativo. Il giurista in questi casi deve partire dalla tradizione e renderla viva nel contesto (piattaforma informatica) di oggi. Alla luce di queste considerazioni, la soluzione sopra riportata, fornita dal Garante nelle LG Referti (sebbene laconica e, a tratti, sibillina), diviene un grimaldello per cercare di risolvere il problema che qui ci impegna: in tale documento si sostiene che l'intermediazione del medico potrebbe essere soddisfatta anche accompagnando la comunicazione dei dati grezzi (il reperto) con un giudizio scritto e con la successiva disponibilità del medico a fornire ulteriori indicazioni.

Da un punto di vista implementativo ciò si traduce, come spiegato, nella predisposizione di una piattaforma che permetta l'accesso da parte del paziente ai dati, prodotti dall'operatore sanitario o dall'azienda in generale, che lo riguardano, forniti di un apparato esplicativo (il più preciso ed approfondito possibile); inoltre, un messaggio potrebbe avvertire il paziente della necessità-opportunità di recarsi dal medico prescrittore per farsi «spiegare» meglio il contenuto dell'esame a cui si è sottoposto. Sebbene tutto questo si traduca in una forzatura dell'espressione testuale «solo per il tramite» di cui all'art. 84 Codice Privacy, risulta anche evidente che la soluzione trova applicazione in un contesto, informatico e culturale, mutato rispetto a quello che ha fatto da substrato all'ideazione di una disposizione normativa così stringente: il paziente, sempre più centro del sistema, non è più, o lo è sempre meno, quell'oggetto passivo, ed ignorante, che si rivolgeva al medico affinché, quasi *deus ex machina*, lo aiutasse nel risolvere il problema che lo angustiava. Egli, invece, acquisisce via via una propria cultura medica (sebbene frammentaria e lacunosa) e scopre, così, le potenzialità che lo strumento informatico gli consente in svariati ambiti del proprio vivere sociale ed, evidentemente, anche con riferimento al proprio stato di salute. Lo strumento digitale diviene così amplificatore piuttosto che freno, o pericolo, della prestazione sanitaria che viene erogata.

Questo genere di considerazioni rimangono purtroppo soluzioni interpretative che forzano il dato normativo ad una mutata realtà. Pur non volendo scadere in scontate istanze positiviste, appare evidente come un chiaro intervento del legislatore in tema di FSE potrebbe sciogliere molti nodi critici dell'intero sistema, i quali divengono ancor più intricati allorché si voglia applicare un armamentario giuridico obsoleto ad uno strumento informatico completamente nuovo[70].

2.9 Informativa e consenso

Le LG FSE riprendono principi oramai assodati nell'ambito del trattamento dei dati sanitari, allorquando affrontano il tema dell'informativa e del consenso[71].

---

[70] Merita almeno un cenno la questione relativa all'opportunità di concedere che l'interessato acceda tramite FSE ai referti che lo riguardano durante il suo stato di ospedalizzazione in occasione di un ricovero. Il problema non rappresenta certo un caso di scuola, stante la diffusione dell'utilizzo dei c.d. *smart phone.* In tale contesto, si potrebbero considerare mutate le esigenze che nella condizione normale consigliano, invece, di permettere all'assistito la fruizione del referto *on-line.* Il semplice fatto che la singola prestazione si caratterizza in quanto parte di un più complesso trattamento sanitario sovrainteso in costanza di ricovero, suggerisce che all'assistito non sia concesso di accedere ai referti ospedalieri prodotti nel mentre egli risulta destinatario della cura: il significato di questi è, infatti, oggetto di comunicazione ed esplicazione da parte del medico curante nell'ambito della relazione terapeutica in atto. Tali considerazioni si ritrovano nei *deliverable* prodotti nell'ambito del progetto «TreC – La Cartella Clinica del Cittadino» e nello specifico in U. IZZO, P. GUARDA, *Parere in merito alla policy da adottare per interpretare le esigenze a cui offre tutela l'art. 84 del Codice Privacy in tema di trasmissione dei referti all'interessato*, 2011.

[71] Per approfondimenti in tema di informativa e consenso in ambito sanitario di cui agli articoli 77-82 Codice Privacy, v. R. JUSO, *Dati sensibili e consenso informato: profili costituzionali e legislativi*, in *Ragiusan*, 2004, fasc. 247/248, 6; C.M. ZAMPI, M. BACCI, G. BENUCCI, L. BALDASSARRI, *Diritto alla salute, diritto alla privacy e consenso dell'avente diritto*, in *Riv. it. medicina legale*, 2001, 1037; CAGGIA, *Il trattamento dei dati sulla salute, con particolare riferimento all'ambito sanitario*, cit., 415-417; RICCIO, *Privacy e dati sanitari*, cit., 265-292; BIANCA, BUSNELLI (a cura di), *La protezione dei dati personali*, cit., art. 77-78, 1224-1267 (commento di A. RENDA); art. 79-

L'informativa, che può anche essere fornita assieme a quella relativa al trattamento dei dati personali, deve evidenziare tutti gli elementi richiesti dall'art. 13 Codice Privacy e descrivere i termini del servizio offerto, sottolineando la sua facoltatività, senza che ciò incida minimamente sulla possibilità di accedere alle cure mediche[72]. Essa deve, inoltre, indicare con formule sintetiche, ma facilmente comprensibili, i soggetti che, nel prendere in cura l'interessato, potranno accedere a tale strumento informatico, nonché la connessa possibilità di acconsentire a che solo alcuni di essi possano consultarlo[73]. Inoltre essa dovrà sicuramente vertere su alcuni ulteriori punti: l'opportunità che tale innovativo strumento offre per migliorare le procedure atte a garantire il diritto alla salute, ma, al tempo stesso, l'ampia sfera conoscitiva che esso può avere; le modalità di funzionamento, almeno nei loro aspetti essenziali, del nuovo strumento digitale; la possibilità che il FSE del paziente venga consultato, anche senza il suo consenso, ma pur sempre nel rispetto dell'autorizzazione generale del Garante Privacy, qualora ciò sia indispensabile per la salvaguardia della salute di un terzo o della collettività (v. art. 76 Codice Privacy); la circostanza che il consenso alla consultazione di un FSE da parte di un determinato soggetto (MMG, PLS, ecc.) possa esser riferito anche al suo sostituto.

Il consenso a questo ulteriore trattamento dei dati sanitari gioca un ruolo rilevantissimo (art. 81 Codice Privacy)[74]. Esso deve necessariamente avere determinate caratteristiche. Sebbene possa essere manifestato unitamente a quello previsto per il trattamento dei dati a fini di cura, tale consenso deve essere autonomo, quindi raccolto *ad hoc*, e specificamente rivolto al trattamento mediante FSE: è questo un consenso generale all'immissione nel FSE dei propri dati, che non esclude,

---

80, 1256-1267 (con commento di M. GAGLIARDI); art. 82, 1268-1291 (con commento di C. FAVILLI); art. 83, 1291-1302 (con commento di M.C. POLO).

[72] LG FSE, p. 8.1, 8.2.

[73] *Ibidem*, p. 8.3.

[74] *Ibidem*, p. 8.1 ss.

ma anzi lascia vivere, una serie di consensi specifici per legittimare la consultazione del fascicolo elettronico da parte dei singoli titolari del trattamento (questa caratteristica va debitamente incorporata all'interno delle funzionalità offerte all'interessato nell'ambito della piattaforma informatica del FSE).

Merita anzitutto di essere sottolineato come, nella sua impostazione base, il FSE concepito dal Garante privilegi la scelta di un sistema di *opt-in*, in linea con l'assetto della normativa sulla protezione dei dati personali. Un sistema di *opt-in*, però, modulare, profilato con riferimento agli specifici dati inseribili all'interno del sistema informativo. Logica conseguenza di ciò è la raccolta di un consenso autonomo e specifico, disgiunto da quello richiesto per il trattamento dei dati raccolti per specifiche finalità di cura; appare, allora, doveroso in questa sede sottolineare come l'ipotizzare che questo adempimento debba avvenire in modalità cartacea – e non, come sarebbe decisamente preferibile, attraverso una registrazione del consenso predisposta in via informatica attraverso la piattaforma utente del FSE (magari in sede di primo accesso del paziente stesso) – esporrebbe il titolare del trattamento legato al FSE ad oneri economici, logistici ed organizzativi piuttosto gravosi.

È del pari evidente che la moltiplicazione dei consensi, in linea con un concetto di autodeterminazione forte e selettiva gestita dall'interessato, prelude necessariamente alla possibilità che tale momento volontaristico, all'interno della piattaforma di gestione del FSE, venga concretamente gestito dall'interessato-paziente attraverso interfacce che permettano a quest'ultimo di esprimerlo o revocarlo in relazione a livelli di accesso modulari (ad esempio, a basi di dati differenziate) da parte di diversi titolari. Il sistema deve anche in questo caso tenere traccia delle opzioni così poste in essere.

Resta da valutare, nel quadro del provvedimento in tema di FSE, l'opportunità di specificare quanto appare reso facoltativo dall'art. 82 Codice Privacy, ovvero che in caso di assoluta necessità dettata

dall'urgenza di salvare l'interessato da un immediato pericolo di vita, sia concesso ad un incaricato identificato dal sistema la possibilità di accedere ai suoi dati sanitari, sebbene manchi una preventiva espressione del consenso a tale operazione. Per quanto riguarda il sistema informativo atto a gestire l'accesso ai dati d'emergenza, si potrebbe ipotizzare una soluzione di questo tipo: il FSE dovrebbe essere in grado di prevedere la possibilità per l'operatore sanitario di accedere a questi dati, auto-certificando i motivi che legittimano tale operazione. Ciò garantirebbe la necessaria flessibilità ed elasticità nell'accesso ai dati sanitari, specie in situazioni di pericolo di vita del paziente, e permetterebbe di porre in essere una verifica *ex post* dei requisiti di fatto e di diritto che hanno obbligato a tale accesso (una soluzione simile è implementata nel DMP francese dove, nei casi di emergenza, è prevista la c.d. *bris de glace* (rottura del vetro, appunto): una procedura che permette l'accesso al FSE quando vi sia l'impossibilità per il paziente di prestare il consenso; il paziente conserva però un controllo *ex post* essendo egli in grado di sapere esattamente chi ha avuto accesso, quando e perché)[75].

2.10 Sintesi dei dati rilevanti

Altro aspetto peculiare del FSE è quello di poter presentare, ove il titolare abbia scelto di dotare il proprio sistema di questa funzionalità, una sintesi di dati clinici rilevanti, indispensabili per salvaguardare la vita dell'interessato: ad esempio la presenza di malattie croniche, di reazioni allergiche, l'utilizzo di dispositivi salvavita, ecc. L'accesso a tali informazioni dovrebbe essere garantito a tutti i soggetti che prendono in cura il paziente (e di questo l'interessato deve essere reso edotto tramite l'informativa *ex* art. 13).

[75] Art. R 161-69-24 del *Code de la Sécurité Sociale*. Se così si disponesse, andrebbe chiarito se tale modalità (con il contrappasso del controllo *ex post* sulla legalità dell'azione intrapresa) possa spingersi a consentire l'accesso ai dati specificatamente oscurati dall'interessato stesso.

Questa sintesi di dati rilevanti deve essere individuata in modo esaustivo dal titolare del trattamento, il quale ha pure l'obbligo di provvedere ad aggiornarne l'elenco[76]. Si tratta del c.d. *patient summary*, definibile come un profilo sintetico in grado di rendere superfluo l'accesso alla documentazione completa per orientare l'inquadramento del paziente oppure per indirizzare l'operatore sanitario nella ricerca delle informazioni pertinenti all'interno del fascicolo[77].

L'individuazione stessa del nucleo di informazioni fondamentali per la salvaguardia dell'incolumità psico-fisica del soggetto rappresenta un problema da affrontare con attenzione. Va osservato che nella logica (che il FSE rende possibile) della documentazione e registrazione degli accessi al dato (magari con informativa automatica all'interessato), l'esigenza di stabilire un *plafond* minimo di dati accedibile in caso di emergenza potrebbe venire ridimensionata a favore dell'idea che, quando l'utente incaricato «rompe il vetro» e attesta di essere legittimato all'accesso dalla circostanza legittimante (la necessità a vantaggio immediato della salute, se non della vita stessa, dell'interessato), quest'ultimo può accedere a qualsiasi dato egli ritenga necessario conoscere.

---

[76] LG FSE, p. 5.18.

[77] Sul *patient summary* v. in prima battuta: A. ROSSI MORI, *Patient Summary e documentazione clinica*, giugno 2007, in Rete: <http://www.sanitaelettronica.cnr.it /lumir_old/rapporti_pdf/pat_sum.pdf>. V. anche il documento a carattere tecnico del TSE, *Specifiche tecniche per la creazione del "Profilo sanitario sintetico" secondo lo standard HL7-CDA Rel. 2*, Versione 1.0, 4 novembre 2010, in Rete: <http://www. innovazionepa.gov.it/media/605046/profilosanitario%20sintetico-cda-1.0.pdf>. Le «Linee guida sul fascicolo sanitario elettronico», proposte dal Ministero della Salute ed approvate dalla Conferenza Stato-Regioni, trattano di «Profilo Sanitario Sintetico» definendolo: «il documento informatico sanitario che riassume la storia clinica del paziente e la sua situazione corrente. Tale documento è creato ed aggiornato dal MMG/PLS ogni qualvolta intervengono cambiamenti da lui ritenuti rilevanti ai fini della storia clinica del paziente e, in particolare, contiene anche un set predefinito di dati clinici significativi utili in caso di emergenza» (p. 13).

2.11 Misure di sicurezza

Il Garante Privacy sottolinea come la delicatezza dei dati personali trattati mediante FSE imponga l'adozione di specifici accorgimenti tecnici per assicurare idonei livelli di sicurezza (art. 31 Codice Privacy), ferme restando le misure minime che ciascun titolare del trattamento deve comunque adottare ai sensi del Codice (artt. 33 ss. Codice Privacy). In considerazione della qualità dei dati che un sistema di FSE tratta, è di tutta evidenza come gli aspetti di sicurezza siano centrali anche e soprattutto per ingenerare il giusto livello di fiducia negli operatori e nei fruitori dell'intera piattaforma[78].

[78] Il quadro normativo di riferimento nell'ordinamento italiano appare ampio e variegato. Esso è, innanzitutto, costituito dall'art. 22 Codice Privacy rubricato «Principi applicabili ai dati sensibili e sanitari». I comma 6 e 7 infatti così recitano: «6. I dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, sono trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità. 7. I dati idonei a rivelare lo stato di salute e la vita sessuale sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo. I medesimi dati sono trattati con le modalità di cui al comma 6 anche quando sono tenuti in elenchi, registri o banche di dati senza l'ausilio di strumenti elettronici». Sempre nel Codice Privacy, troviamo poi l'art. 34, co. 1, lett. h, che impone «l'adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari», e l'Allegato B del Codice «Disciplinare tecnico in materia di misure minime di sicurezza», che prevede i requisiti che un sistema informativo deve implementare tra i quali quelli di cui al punto 24: «Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di cui all'articolo 22, co. 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. I dati relativi all'identità genetica sono trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato». Nel

Le LG FSE prevedono espressamente gli aspetti relativi alla sicurezza informatica che devono essere necessariamente incorporati nella piattaforma:

- idonei sistemi di autenticazione e di autorizzazione per gli incaricati in funzione dei ruoli e delle esigenze di accesso e trattamento (ad es., in relazione alla possibilità di consultazione, modifica e integrazione dei dati);
- procedure per la verifica periodica della qualità e coerenza delle credenziali di autenticazione e dei profili di autorizzazione assegnati agli incaricati;
- individuazione di criteri per la cifratura o per la separazione dei dati idonei a rivelare lo stato di salute e la vita sessuale dagli altri dati personali;
- tracciabilità degli accessi e delle operazioni effettuate;
- sistemi di *audit log* per il controllo degli accessi al database e per il rilevamento di eventuali anomalie[79].

L'adozione di un sistema di autenticazione «sicuro» appare un aspetto cruciale per una piattaforma di FSE[80]. Il Documento di lavoro

contesto italiano vanno poi ricordate l'Autorizzazione n. 2/2009 al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale del 16 dicembre 2009 e l'Autorizzazione generale del Garante al trattamento dei dati genetici del 22 febbraio 2007, ulteriormente differita il 22 dicembre del 2009 (v. Ulteriore differimento dell'efficacia dell'Autorizzazione al trattamento dei dati genetici rilasciata il 27 aprile 2010). Vi sono poi fonti internazionali, le quali, sebbene non dotate di carattere cogente, trovano applicazione in materia. Ci riferiamo alla Raccomandazione R (97) 5 del Consiglio d'Europa, relativa alla protezione dei dati sanitari, ed al «Documento di lavoro sui dati genetici» adottato il 17 marzo 2004 dal Gruppo Articolo 29. In tema di sanzioni penali per illecito trattamento dei dati sanitari, v., anche se datato, C. SARZANA DI S. IPPOLITO, *Responsabilità penali connesse al trattamento ed all'uso dei dati sanitari*, in *Dir. pen. e proc*., 2002, 903.

[79] LG FSE, p. 10.3.

[80] Nel romanzo M. FIORANELLI, P. ZULLINO, *Io, Ippocrate di Kos*, Roma-Bari, 2009 a pagina 42 gli autori fanno pronunciare al mitico fondatore dell'arte medica una frase sicuramente calzante al tema oggetto qui di approfondimento: «Questa degli impostori è una piaga che dovrà affliggerci fino a quando i governi non avranno trovato il modo

CCE Gruppo art. 29 nella parte terza («Riflessioni su un quadro giuridico adatto per i sistemi di CCE») tratta di «Identificazione e riconoscimento dei pazienti e del personale sanitario» e sottolinea come

> l'identificazione affidabile dei pazienti nei sistemi CCE è di fondamentale importanza. L'utilizzo di dati sulla salute relativi alla persona sbagliata, a causa di un errore di identificazione, può avere conseguenze spesso nefaste.

Più avanti nello stesso testo si legge

> dato il carattere particolarmente delicato dei dati sulla salute le persone non autorizzate non devono potervi accedere. Un controllo affidabile dell'accesso dipende da un'affidabile identificazione e riconoscimento. Per questo è indispensabile identificare inequivocabilmente gli utilizzatori e anche riconoscerli correttamente[81].

La soluzione proposta dal Gruppo articolo 29, che si ritrova tra l'altro in alcuni esperimenti italiani a livello regionale, è rappresentata dall'utilizzo di *smart card* che garantiscano un elevato livello di affidabilità e sicurezza:

> Le tessere sanitarie basate sul sistema delle *smart card* potrebbero contribuire in maniera significativa a una corretta identificazione elet-

---

di provare le identità personali. Oggi chiunque si presenta tra due comparti che gli reggono il gioco e dice "sono il Tale" e può essere creduto. Chiunque scrive lettere e si firma col nome di chiunque: puoi cascarci. Nella posta ci affidiamo agli anelli-sigillo che imprimono il nostro logo sulla ceralacca, ma è ben poco, perché si possono falsificare. Qualcuno ha escogitato codici di sicurezza: ad esempio, se nella terza e terzultima riga del testo risulta scritta una stessa parola, la lettera che stai leggendo è proprio mia. Ma è arzigogolo da uomini politici. Da servizi segreti, da avvocato. Mica da gente comune».

[81] Documento di lavoro CCE Gruppo art. 29, 15.

tronica dei pazienti e anche al loro riconoscimento se vogliono accedere ai dati della loro CCE[82].

I sistemi informativi prevedono l'uso di dispositivi per verificare l'identità digitale dell'utente prima di autorizzarne l'accesso alle risorse presenti nei diversi domini di cui essi si compongono. Nel nostro caso sarebbe, quindi, opportuno affiancare all'attribuzione al cittadino di *login* e *password* l'erogazione anche di una *smart card*. Questa può essere rappresentata dalla più volte promessa, ma mai pienamente realizzata a livello nazionale, «Carta d'Identità Elettronica (CIE)», consistente in una carta a microprocessore con caratteristiche del documento di riconoscimento «a vista» affiancate a requisiti di sicurezza fisica (banda ottica, ologrammi, foto del titolare), o dalla «Carta Nazionale dei Servizi (CNS)», una *smart card* progettata per consentire l'accesso ai servizi *on-line* della pubblica amministrazione[83].

In ogni caso il trattamento di dati sanitari tramite sistemi di FSE deve basarsi sull'utilizzo di standard crittografici per la comunicazione elettronica dei dati tra i vari titolari coinvolti[84].

2.12 Una nuova frontiera: piattaforme Personal Health Record *e dati inseriti direttamente dal paziente*

L'ultima frontiera della gestione informatizzata dei dati sanitari è rappresentata dalle piattaforme che permettono una più incisiva partecipazione del paziente-utente (PHR), il quale diviene così attore protagonista nella determinazione dei flussi informazionali e, di conseguenza, dei percorsi curativi che lo riguardano. Tale aspetto è stato più volte in precedenza sottolineato e posto all'attenzione del lettore. In questo

[82] *Ibidem*, 14.
[83] V. art. 66 «Carta d'identità elettronica e carta nazionale dei servizi» CAD.
[84] LG FSE, p. 10.4.

paragrafo si intende approfondire la questione fornendo alcuni utili spunti di riflessione.

Le possibilità offerte al paziente con questo tipo di strumenti possono variare e si connotano di diverse funzionalità. Certamente la loro implementazione non può che avvenire per fasi: questo al fine di permettere all'utente di impratichirsi con il nuovo servizio, di familiarizzare con le nuove forme di interazione umane e professionali che esso determina e per consentire la risoluzione di problemi e difficoltà che l'utilizzo di piattaforme informatiche, di per sé rigide e non tanto elastiche quanto la complessità giuridica richiederebbe.

Innanzitutto, il paziente avrà la possibilità di immettere dati che lo riguardano all'interno del proprio FSE. Egli andrà, così, ad alimentare quell'isola di dati a cui sopra si è fatto cenno, la cui gestione, pur facendo essi parte del *dossier* aziendale e quindi sotto la titolarità di tale ente, sarà interamente sotto il suo controllo e, quantomeno nella prima fase di implementazione, accessibile solamente a lui. Ciò gli permetterà un accesso alla piattaforma più «fidelizzante» e gli consentirà di utilizzare lo strumento offerto come un diario personale della propria salute, su cui memorizzare auto-misurazioni, terapie farmaceutiche, sintomatologie. Non è peregrino ritenere, poi, che, con particolare riferimento ai malati in acuzie o cronici, queste autovalutazioni possano essere in un secondo momento affiancate da misurazioni, invece, a carattere oggettivo poste in essere da apparecchiature certificate dall'azienda, installate nell'abitazione del paziente e controllate da remoto. Le informazioni contenute in questa isola di dati del cittadino possono essere rese disponibili anche all'interno dell'azienda sanitaria. La piattaforma può, inoltre, fungere da punto d'accesso per i referti clinici relativi ad esami o prove di laboratorio cui il paziente si è sottoposto. Ci riferiamo alla c.d. refertazione *on-line* di cui si darà descrizione a momenti, che è stata oggetto di analisi da parte del Garante Privacy nelle LG Referti.

Stante la definizione che il Garante ha fornito nelle LG FSE, i trattamenti sopra descritti rientrano ancora nell'ambito di un *dossier* aziendale, il quale, giova qui ricordarlo nuovamente, viene definito come uno strumento

> costituito presso un organismo sanitario in qualità di unico titolare del trattamento (es., ospedale o clinica privata) al cui interno operino più professionisti[85].

Ancora non si determina nei passaggi descritti quella «condivisione logica» di cui parla il Garante sempre nelle LG FSE:

> insieme dei diversi eventi clinici occorsi ad un individuo messo in condivisione logica dai professionisti o organismi sanitari che assistono l'interessato, al fine di offrirgli un migliore processo di cura[86].

E certamente non si concretizza la più specifica figura di FSE, ricordiamolo, definita come

> fascicolo formato con riferimento a dati sanitari originati da diversi titolari del trattamento operanti più frequentemente, ma non esclusivamente, in un medesimo ambito territoriale (es., azienda sanitaria, laboratorio clinico privato operanti nella medesima regione o area vasta)[87].

Tale ulteriore passaggio si compie allorquando l'isola di dati del cittadino ed il suo diario personale vengono messi in condivisione anche con gli incaricati della ASL, i MMG, i PLS e le strutture convenzionate esterne all'azienda. In questo momento, controllato dal paziente, si determina un'interconnessione tra banche dati gestite da diversi ed

[85] LG FSE, p. 2.4. Il servizio viene offerto dall'azienda sanitaria e, quindi, rientra pienamente sotto il suo controllo e gestione e, di conseguenza, sotto la sua titolarità.

[86] *Ibidem*, p. 1.5.

[87] *Ibidem*, p. 1.4.

autonomi titolari dei rispettivi trattamenti. Si innescano, allora, le problematiche tipiche dei FSE e sorgono i problemi di titolarità ed eventuale co-titolarità con riferimento al trattamento dei dati.

Questi servizi, che rappresentano la nuova frontiera della sanità elettronica, condizioneranno e modificheranno le relazioni interpersonali tra i soggetti coinvolti (paziente, medico, azienda, ecc.) ed il rapporto stesso tra il cittadino-interessato ed i propri dati clinici.

3. La documentazione sanitaria

Particolare attenzione dev'essere riservata alla tipologia di dati che possono essere trattati attraverso il FSE ed alla granularità dell'accesso a questi. Ricordando quanto disposto dal Codice Privacy agli artt. 11, co. 1, lett. d) e 22, co. 5, il Garante sottolinea come la regola aurea da seguire debba essere quella dell'attenta valutazione circa la pertinenza, la non eccedenza e la rilevanza dei dati da inserire nel FSE con riferimento alle finalità di prevenzione, diagnosi, cura e riabilitazione[88].

[88] *Ibidem*, p. 5.1. Occorre anche tenere presente un ulteriore passaggio delle LG già citato in una precedente nota e che qui si riporta per chiarezza (p. 5.6): «I titolari del trattamento, nel costituire il Fse/*dossier* e nell'individuare la tipologia di informazioni che possono esservi anche successivamente riportate, devono rispettare le disposizioni normative a tutela dell'anonimato della persona tra cui quelle a tutela delle vittime di atti di violenza sessuale o di pedofilia (l. 15 febbraio 1996, n. 66; l. 3 agosto 1998, n. 269 e l. 6 febbraio 2006, n. 38), delle persone sieropositive (l. 5 giugno 1990, n. 135), di chi fa uso di sostanze stupefacenti, di sostanze psicotrope e di alcool (d.P.R. 9 ottobre 1990, n. 309), delle donne che si sottopongono a un intervento di interruzione volontaria della gravidanza o che decidono di partorire in anonimato (l. 22 maggio 1978, n. 194; d.m. 16 luglio 2001, n. 349), nonché con riferimento ai servizi offerti dai consultori familiari (l. 29 luglio 1975, n. 405). Il titolare del trattamento può, pertanto, decidere di non inserire tali informazioni nel Fse/*dossier*, ovvero di inserirle a fronte di una specifica manifestazione di volontà dell'interessato, il quale potrebbe anche legittimamente richiedere che tali informazioni siano consultabili solo da parte di alcuni soggetti dallo stesso individuati (ad es. specialista presso cui è in cura)».

La valutazione dei dati clinici da inserire nel FSE non rappresenta certo una scelta di poco momento. La documentazione sanitaria è caratterizzata dalla presenza di numerose tipologie di informazioni. Possiamo così avere: la cartella clinica; la cartella infermieristica (un supporto documentativo non obbligatorio per la pianificazione dell'assistenza); la refertazione (ivi compresa quella di pronto soccorso); l'analisi di laboratorio; le moderne metodiche di *imaging*; l'informazione al medico curante ed agli interessati («lettera di dimissione ospedaliera»); le certificazioni e le prescrizioni sanitarie; i dati rilevati ed inseriti direttamente dal paziente (nuova frontiera dei sistemi PHR).

In questa massa di dati vanno accuratamente individuate le informazioni strettamente necessarie alle finalità di cui si connota il FSE. Va, poi, valutato il livello modulare di accesso alla luce del più volte richiamato principio di autodeterminazione dell'interessato. È, quindi, chiaro come il momento della definizione delle regole di gestione del FSE rappresenti un aspetto cruciale: le esigenze del singolo paziente vanno armonizzate e coordinate con le regole interne proprie della struttura sanitaria (anche con riferimento al rispetto del *need to know* interno, inerente ai livelli di accesso dei singoli incaricati dalla struttura titolare) e con le imprescindibili esigenze terapeutiche[89].

Possiamo definire la categoria «documentazione sanitaria» come l'insieme di tutte le svariate forme di comunicazione, scritta o orale, che mettono in relazione il paziente con il professionista sanitario e con la struttura sanitaria stessa[90]. Dal punto di vista dei contenuti si può, poi, parlare di documentazione sanitaria «informativa»; ad esempio, nel

[89] Nell'analisi dei diversi documenti che caratterizzano i flussi informativi della sanità moderna occorre tenere in considerazione il fatto che, con l'avvio di progetti che porteranno ad una loro completa gestione digitale, probabilmente non avrà più molto senso differenziare tra paziente ricoverato e paziente ambulatoriale.

[90] Si prenda a riferimento come studio analitico-descrittivo della documentazione sanitaria S. CORONATO, *La documentazione sanitaria in ospedale*, in *Ragiusan*, n. 267/268, 2006, 24; v. anche B. MAGLIONA, *Documentazione sanitaria (conservazione e archiviazione),* in *Digesto pen.*, Torino, 1990, vol. IV, 169.

caso di un'informazione sui farmaci o di quella fornita dal medico ospedaliero al medico curante del paziente dimesso o di quella «prescrittiva», come ad esempio la ricetta relativa ad un farmaco.

Vediamo di seguito una breve descrizione di queste forme di comunicazioni che l'ambito medico-ospedaliero.

3.1 Cartella clinica

Documento principe nell'universo del sistema informativo ospedaliero è la «cartella clinica»[91]. Tale strumento è nato per garantire che l'esigenza di raccolta e trasmissione dei dati clinici relativi ad un ricovero ospedaliero fosse soddisfatta.

Prima di passare all'analisi di questo tipo di documento sanitario, è opportuno sgomberare il campo da un possibile fraintendimento terminologico. Spesso si sente parlare – più in passato a dire il vero, cioè prima che il Garante Privacy intervenisse con un provvedimento *ad hoc* – di «cartella clinica digitale», ingenerando una sorta di confu-

[91] Cfr. P. BAICE, *La cartella clinica tra diritto di riservatezza e diritto di accesso*, in *Resp. civ*., 2008, 169; F. FRÈ, *La cartella clinica nel sistema sanitario italiano*, in *Nuova rass. legislazione, dottrina e giurisprudenza*, 2007, fasc. 23-24, 2387; F. TOSI, *La tutela della riservatezza nei codici di deontologia professionale del medico e dell'infermiere, privacy e cartella clinica*, in *Sanità pubblica*, 2006, 60; B. PRIMICERIO, *La cartella clinica e la documentazione sanitaria ad essa collegata: evoluzione, utilizzazione e responsabilità*, in *Il Diritto sanitario moderno*, 2004, 207; V. VACCARO, *La cartella clinica* (Nota a TAR VE sez. III 7 marzo 2003, n. 1674), in *Trib. am. reg*., 2003, 180; G. ROCCHIETTI, *La documentazione clinica. Compilazione, conservazione, archiviazione, gestione e suo rilascio da parte della direzione sanitaria. Trattamento dei dati sanitari e privacy,* in *Minerva medicolegale*, 2001, fasc. 1, 15; O. BUCCI, *La cartella clinica. Profili strumentali, gestionali, giuridici ed archivistici*, Santarcangelo di Romagna, 1999; E. BARILÀ, C. CAPUTO, *Problemi applicativi della legge sulla privacy: il caso delle cartelle cliniche*, in *Politica del diritto*, 1998, 275; F. BUZZI, C. SCLAVI, *La cartella clinica: atto pubblico, scrittura privata o "tertium genus"?*, in *Riv. it. medicina legale*, 1997, 1161; A. BASSI, *La cartella clinica come atto amministrativo*, in *Dir. ed economia assicuraz.*, 1992, 753; U. GABRIELLI, *La cartella clinica ospedaliera*, in *Riv. it. diritto sociale*, 1970, 498.

sione tra questa e la cartella clinica tradizionale. Appare, invece, concettualmente più corretto riferirsi alle nuove frontiere di gestione informatizzata dei dati sanitari con il termine di FSE, in quanto tale locuzione dissipa qualsiasi dubbio di una possibile, errata, sovrapposizione contenutistica con il già noto documento cartaceo. Il nuovo strumento, infatti, modifica le categorie organizzative stesse della documentaristica sanitaria costituendo un contenitore più ampio di dati relativi alla storia clinica di un paziente e garantendogli un livello di interoperabilità e di coinvolgimento sconosciuti in passato.

Non esiste, a livello normativo, una definizione a carattere generale di cartella clinica, nemmeno con riferimento al suo mero contenuto né alle modalità di redazione e compilazione. Occorre quindi rifarsi a normative di carattere settoriale ed al significato, attribuitogli nella prassi, di

> documentazione relativa alle condizioni di salute di una persona ricoverata in ospedale o sottoposta ad analisi e cure mediche[92].

La normativa di riferimento è contenuta nel d.m. Sanità 5 agosto 1977 «Requisiti delle case di cura private», nel d.p.c.m. 27 giugno 1986 «Atto di indirizzo e coordinamento dell'attività amministrativa delle regioni in materia di requisiti delle case di cura private», e nella circolare del Ministero della sanità n. 900.2/2.7/190 del 14 marzo 1996. Questo sistema di fonti prevede che per ogni singolo ricoverato sia compilata una cartella clinica da cui devono risultare le generalità complete, la diagnosi di ingresso, l'anamnesi familiare e personale, l'esame obiettivo, gli esami di laboratorio e specialistici, la diagnosi, la terapia, gli esiti e i postumi.

[92] In BAICE, *La cartella clinica tra diritto di riservatezza e diritto d'accesso*, cit., 169.

Altro testo di riferimento è il «Codice di deontologia medica» dove, all'art. 23, si rinvengono i requisiti circa la sua compilazione:

> la cartella clinica deve essere redatta chiaramente, con puntualità e diligenza, nel rispetto delle regole della buona pratica clinica e contenere, oltre a ogni dato obbiettivo relativo alla condizione patologica e al suo decorso, le attività diagnostico-terapeutiche praticate.

Si può allora definire la cartella clinica come un insieme di informazioni e documenti che registrano i dati anagrafici e sanitari di una persona[93].

Tale strumento ha come scopo precipuo quello di garantire la raccolta dei dati relativi ad ogni singolo ricovero. Essa svolge le seguenti funzioni: fornire una base informativa, consentire la tracciabilità delle attività svolte, facilitare l'integrazione di competenze multiprofessionali, costituire una fonte informativa per ricerche clinico-scientifiche, formazione degli operatori, studi valutativi ed esigenze amministrative e gestionali[94].

---

[93] Il tema della natura giuridica della cartella clinica ha impegnato la dottrina e la giurisprudenza per molti anni e, ad oggi, non si può dire che si sia giunti ad una visione condivisa: cfr. FRÈ, *La cartella clinica nel sistema sanitario italiano*, cit., 2388. Senza analizzarne in questa sede i particolari che esulano dal nostro ambito di indagine, basti rilevare che il dibattito vedeva da un lato la tesi che sosteneva la natura di atto pubblico della cartella clinica, in quanto essa determinerebbe effetti incidenti su situazioni giuridiche soggettive di rilevanza pubblicistica e documenterebbe attività compiute da un pubblico ufficiale (v. la Circolare del Ministero della sanità n. 900.2/A.G. 464/260 del 19 dicembre 1986, che ribadisce che «le cartelle cliniche rappresentano un atto ufficiale indispensabile a garantire la certezza del diritto»), dall'altro la posizione volta a limitare il valore probatorio di atto pubblico esclusivamente alle attestazioni relative all'attività espletata nel corso delle attività cliniche, attribuendo a queste ultime lo *status* di prove privilegiate e non riconoscendo, invece, alle diagnosi in essa contenute alcun valore privilegiato rispetto ad altri elementi di prova: cfr. Cass., sez. III, 27 settembre 1999, n. 10695, in *Gazzetta giur*., 1999, fasc. 40, 38. V. anche sul diverso valore assegnato alle fasi di compilazione della cartella clinica rispetto alla sua chiusura Cass., sez. V, 8 febbraio 1991, in *Mass. Cass. pen*., 1991, fasc. 5, 12 (m).

[94] Cfr. FRÈ, *La cartella clinica nel sistema sanitario italiano*, cit., 2389.

Aspetto problematico di questo strumento, anche in prospettiva di una sua graduale digitalizzazione, è quello collegato alla conservazione ed alla archiviazione. L'art. 22, co. 6, Codice Privacy stabilisce che:

> I dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, sono trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità.

Con specifico riferimento alle cartelle cliniche, sempre il Codice Privacy prevede l'obbligo di adottare opportuni accorgimenti per assicurare la comprensibilità dei dati e per distinguere quelli relativi al paziente da quelli riguardanti altri interessati (art. 92, co. 1). Al fine di stabilire la durata prevista per la conservazione della cartella clinica, occorrerebbe che il legislatore intervenisse chiarendo in maniera definitiva la questione. Sulla base, invece, del nostro attuale assetto normativo, occorre delineare alcune distinzioni. Se si privilegia il fatto che l'ente tenuto alla conservazione della cartella clinica debba essere l'azienda sanitaria, allora è opportuno fare riferimento alla normativa settoriale, la quale dispone l'obbligo di conservazione integrale, per i primi quarant'anni, in un archivio corrente e, successivamente, in una separata sezione. L'obbligo non si riferisce alla documentazione diagnostica, per la quale il limite di conservazione è fissato, invece, in vent'anni (Circolare del Ministero della salute del 19 dicembre 1986, n. 61[95]). Se ci si vuole riferire ad un ambito più generale, sarà necessario

[95] Ove si legge: «le cartelle cliniche, unitamente ai relativi referti, vanno conservate illimitatamente, poiché rappresentano un atto ufficiale del diritto oltre a costituire preziosa fonte documentaria per le ricerche di carattere storico-sanitario».

adeguarsi all'ordinario obbligo di conservazione del materiale archivistico: il termine di conservazione sarà allora quarantennale (art. 30, co. 4, d.lgs. 22 gennaio 2004, n. 42)[96].

Significativa appare in questa diatriba la posizione assunta dal Garante Privacy che, chiamato a pronunciarsi sul rapporto tra l'obbligo di conservazione illimitata delle cartelle cliniche da parte di una casa di cura privata ed il diritto di ottenere la cancellazione dei dati fatto valere dall'interessato al trattamento, ha stabilito la prevalenza della conservazione illimitata, richiamando espressamente la circolare sopra citata[97].

3.2 Cartella infermieristica

La cartella infermieristica è uno strumento che si avvale di un supporto cartaceo e/o informatico, volto a contenere la registrazione dei dati e l'insieme dei documenti di pertinenza infermieristica sul caso oggetto di cura. Essa svolge anche funzioni di certificazione ed organizzazione di tutto il patrimonio informativo e delle attività assistenziali della persona, raccolte e/o eseguite dall'infermiere, favorendone, quindi, la responsabilizzazione. Questo tipo di documento nasce come realizzazione del principio professionale contenuto nel codice deontologico degli infermieri, il quale richiede di assicurare la garanzia delle informazioni relative al piano di assistenza e la continuità assistenziale del paziente, anche e soprattutto mediante una gestione efficace degli strumenti informativi. Il nucleo centrale è caratterizzato dal piano di assistenza personalizzato. Essa viene, quindi, utilizzata per la redazione di anamnesi, la definizione degli obiettivi assistenziali, l'annotazione degli interventi effettuati e la valutazione dei risultati.

---

[96] Diversa possibile soluzione è infine quella di tener conto del termine di prescrizione previsto dall'ordinamento in ordine ad eventuali azioni giudiziarie che qualcuno potrebbe intraprendere.

[97] Garante Privacy, *Decisione su ricorsi*, 13 luglio 2006, in *Boll*., n. 74, 2006, 0.

La cartella clinica infermieristica non è obbligatoria come la cartella clinica nelle strutture ospedaliere, ma, laddove presente, va a costituire parte integrante di quest'ultima.

Da un punto di vista giuridico, essa è stata formalmente riconosciuta dall'art. 69 del d.P.R. 28 novembre 1990, n. 384 e viene considerata come un atto pubblico, in quanto compilata da un incaricato di pubblico servizio.

3.3 Refertazione

La refertazione consiste in quella particolare forma di certificazione atta ad attestare una determinata situazione sanitaria in un dato momento, sotto la responsabilità del professionista che provvede a redigerla[98].

[98] L'importanza di tale assunzione di responsabilità è anche dimostrata dalla previsione in sede penale di specifiche fattispecie criminali: gli artt. 365 e 384 del Codice Penale, infatti, puniscono con sanzioni pecuniarie quei professionisti sanitari che, nell'esercizio della loro professione, abbiano prestato la propria assistenza o opera in casi che possono presentare i caratteri di un delitto per il quale si debba procedere d'ufficio e abbiano omesso o ritardato di riferirlo all'autorità giudiziaria. Ci si riferisce più in particolare ai «referti di pronto soccorso», i quali riguardano prestazioni sanitarie di urgenza attivate dai medici in servizio presso un pronto soccorso ospedaliero. Assumono una notevole rilevanza in quanto contengono gli estremi utili a procedere contro coloro che hanno arrecato danno ad altri soggetti. Per approfondimenti v. G. FINOCCHIARO, *La firma sul referto di laboratorio*, in *Sanità pubbl. e privata*, 2009, fasc. 3, 5; M. TIZIAN, *Aspetti giuridici dell'acquisizione del referto come notizia di reato*, in *Riv. giur. polizia*, 2005, 679; C. LAZZARI, *La guida in stato di ebbrezza tra modalità di accertamento del tasso alcolemico e il reato di omissione di referto ai sensi dell'art. 365 c.p.* (Nota a Giudice di pace Terni, 4 marzo 2003, Paolantoni), in *Rass. giur. umbra*, 2003, 217; V. FINESCHI, E. TURILLAZZI, *Automatismo o discrezionalità nella trasmissione del referto medico: quale risposta dalla recente giurisprudenza?*, in *Riv. it. medicina legale*, 2002, 291; M. TIZIAN, *Obbligo di referto e lesioni personali*, in *Riv. giur. polizia*, 2001, 373; R. BLAIOTTA, *Appunti sul dolo alla luce della recente giurisprudenza di legittimità sul reato di omissione di referto* (Nota a Cass., sez. fer., 8 settembre 1998, Messori), in *Cass. pen.*, 2000, 1242; P. ROSSI, *Denuncia o referto: obblighi del medico operante in «struttura pubblica» ed in particolare nell'Inail*, in *Riv. it. medicina*

Il referto rappresenta la fase finale del processo diagnostico: in esso si ritrova l'analisi critica del risultato di un esame strumentale, di un'analisi di laboratorio o di un esame radiologico (reperto), contenendo talvolta l'interpretazione clinica dei medesimi.

Occorre, inoltre, indicare due tipologie di atti nettamente differenti tra loro nell'ambito della refertazione. Da un lato abbiamo, infatti, il semplice esito degli esami diagnostici eseguiti mediante strumentazioni cliniche (ad es. istopatologia, citologia, ecc.); esito che può esulare del tutto da una qualsiasi interpretazione o valutazione clinica da parte del personale medico. Il Garante Privacy lo chiama «reperto» nelle LG Referti. Dall'altro abbiamo il referto vero e proprio, cioè l'atto scritto con il quale il medico o il tecnico di laboratorio dichiarano conformi a verità i risultati degli esami diagnostici ottenuti, fornendo inoltre un'interpretazione clinica degli stessi, avendo a riferimento il quadro clinico e l'anamnesi del paziente. La sottoscrizione del referto viene anche chiamata «validazione».

Le ultime frontiere degli esami di diagnostica per immagini si sono giovate dell'evoluzione tecnica delle moderne metodiche di *imaging* medico-sanitaria[99].

---

legale, 1997, 917; M. PORTIGLIATTI BARBOS, *Referto e denuncia*, in *Digesto pen*., Torino, 1997, vol. XII, 37; L. FIORAVANTI, *Referto (omissione di)*, *ibidem*, 21; G.A. NORELLI, A. MENCARELLI, G. FRAVOLINI, E. MAZZEO, *L'obbligo di denuncia e di referto nella legislazione e nella prassi sanitaria*, in *Assistenza soc*., 1995, I, 279; O. DE PIETRO, *Il sanitario ed il referto - Rilievi giuridici e medico legali*, Napoli, 1981.

[99] In un futuro non così distante la netta divisione, anche normativa, tra referto ed immagine radiologica potrebbe essere oggetto di un ripensamento. Nella letteratura di settore si comincia a parlare di «referto strutturato» (*structured report*, SR): questo consiste in una commistione tra testo del referto ed immagini correlate e ritenute clinicamente rilevanti per la diagnosi. Il fenomeno comune nell'era digitale del superamento degli antichi confini concettuali caratterizza anche quest'aspetto della documentaristica sanitaria: la gestione elettronica delle informazioni, infatti, sbiadisce il significato del rapporto testo-immagini (carta-pellicole), fondendole di fatto in oggetti della stessa natura (ovvero *bit*), in cui il tradizionale testo lascia il posto al moderno «ipertesto».

3.4 Certificazioni e prescrizioni sanitarie

L'attività di certificazione è caratterizzata dalla compresenza di interessi, talvolta non univoci, tra le esigenze della pubblica autorità e le necessità dei privati. Il potere certificatorio è riservato al medico.

La certificazione agisce in due sensi: da un lato è spesso il privato cittadino ad avere la necessità di una certificazione positiva del suo stato di salute (v. ad es. il «certificato di sana e robusta costituzione»); dall'altro lato, in altre ipotesi l'esigenza sarà di avere la prova di uno stato patologico che giustifichi il paziente in determinate situazioni (ad es. certificato del medico di famiglia da presentarsi al datore di lavoro per un'assenza dovuta a malattia).

Le scelte del medico, poi, con riferimento all'applicazione ed alla programmazione dell'*iter* presso i presidi diagnostici e terapeutici, si estrinsecano nella redazione di «ricette mediche»[100]: queste rappresentano il documento al quale viene affidata la prescrizione farmaceutica rappresentata dall'indicazione del farmaco, della sua posologia e, ove necessario, della sua modalità di somministrazione. La prescrizione medica può tradursi anche nell'individuazione della necessità o dell'opportunità di sottoporsi ad ulteriori prestazioni diagnostiche specialistiche.

Sul tema del rapporto tra diritto alla privacy e prescrizioni mediche, il Codice Privacy, agli artt. 87 e 88, prevede una regolamentazione modulata a seconda che la spesa sia a carico del SSN o meno[101].

---

[100] Per approfondimenti v. M.C. TIRALTI, L. PERIOLI, V. AMBROGI, C. ROSSI, *Aspetti normativi della ricetta medica*, in *Rass. dir. farmaceutico*, 2004, 7; A. FIORI, G. LA MONACA, *Le regole doverose di condotta nel rilascio della ricetta medica* (Nota a Trib. Milano, 25 giugno 1997), in *Riv. it. medicina legale*, 1999, 325; P. MINGHETTI, L. SANFILIPPO, *Formalismi nella redazione e nella documentazione della spedizione delle ricette mediche non ripetibili*, in *Ragiufarm*, 1994, fasc. 19, 4; O. BOSSI, *La ricetta medica dopo il d.lgs. n. 178 del 1991*, in *Rass. dir. farmaceutico*, 1992, 373.

[101] Per maggiori analisi v. BIANCA, BUSNELLI (a cura di), *La protezione dei dati personali*, cit., art. 87 e 88, 1331-1345 (con commento di F. BORGHI).

Nel primo caso, infatti, essa dovrà essere redatta secondo il modello ministeriale, il quale consente l'offuscamento dei dati anagrafici dell'interessato (con la possibilità di svelare tali informazioni solo qualora vi sia l'opportunità di un controllo sulla correttezza della prescrizione); nell'altro caso, invece, il medico dovrà astenersi dall'indicare le generalità del paziente, a meno che ciò non appaia indispensabile.

Si può, da ultimo, menzionare il c.d. «certificato di assistenza al parto», il quale costituisce uno strumento per le rilevazioni dei dati di base concernenti le nascite e dei dati relativi ai nati affetti da malformazioni congenite o ai nati morti[102]. Deve essere redatto entro e non oltre il decimo giorno dalla nascita da parte dell'ostetrica o del medico che ha assistito al parto o, ancora, dal medico responsabile dell'unità operativa in cui questo è avvenuto. Il Codice Privacy, all'art. 93, prevede che per le dichiarazioni di nascita il certificato di assistenza al parto venga sempre sostituito da una semplice attestazione dei dati richiesti nei registri di nascita. Per la rilevazione dei dati statistici relativi alle nascite continuano ad essere osservate le disposizioni impartite dal d.m. 16 luglio 2001, n. 349 del Ministero della salute, nonché le modalità tecniche stabilite dall'Istituto nazionale di statistica (v. art. 109).

3.5 Informazioni agli interessati ed al medico curante

Si è già avuto modo di dimostrare come la cura corrisponda all'apparato informativo costruito attorno al paziente. Lo scambio informazionale rappresenta, anzi, il momento fondamentale del rapporto medico-paziente che costituisce il cuore di qualsiasi processo curativo. Può, così, avvenire che il medico consegni al paziente una relazione firmata nella quale vengono brevemente descritte le diverse proposte

[102] *Ibidem*, art. 93, 1390-1403 (commento di C.M. BIANCA); MONDUCCI, PASETTI, *Il trattamento dei dati sanitari e genetici (Parte II – Titolo V)*, cit., 281-282.

diagnostiche e terapeutiche, le eventuali prospettive ed alternative, i rischi ed i benefici che si possono ragionevolmente attendere.

Come si è già diffusamente rilevato, questo tipo di attività deve conformarsi al dettato dell'art. 84 Codice Privacy, che prevede la disciplina di riferimento per quanto concerne la comunicazione di dati sanitari all'interessato al trattamento, stabilendo la necessaria presenza di un filtro (il professionista sanitario) tra il dato grezzo ed il paziente.

Un'altra tipologia di informazione scritta che assume un ruolo fondamentale da un punto di visto clinico-sanitario è rappresentata dalla c.d. «lettera di dimissione ospedaliera»[103]. Questo documento, trasmesso dalla struttura sanitaria al medico curante oppure al medico di famiglia, deve contenere la diagnosi di dimissione e l'elenco di tutte le più importanti attività cliniche poste in essere durante il ricovero ospedaliero assieme ad un resoconto dettagliato degli eventuali interventi effettuati in tale lasso di tempo. Da un punto di formale, essa deve essere compilata e redatta in forma dattilografata (ovvero scritta al computer) e consegnata all'atto della dimissione al paziente stesso in una busta chiusa (misura di sicurezza nel contesto reale-cartaceo) indirizzata al medico curante.

4. La refertazione on-line*: approfondimento*

Sono stati elencati sopra gli atti normativi ed i documenti, a livello nazionale ed internazionale, tesi ad analizzare le problematiche giuridiche generate dall'implementazione di sistemi di FSE. Nel dare

[103] Per approfondimenti v. M. NONIS, G. CORVINO, A. FORTINO, *La scheda di dimissione ospedaliera. Manuale pratico di compilazione ed uso dello strumento informativo per la classificazione dei ricoveri per DRG/ROD*, Roma, 1997. V. anche il documento a carattere tecnico del TSE, *Specifiche tecniche per la creazione della "Lettera di Dimissione Ospedaliera" secondo lo standard HL7-CDA Rel. 2*, Versione 1.0, 4 novembre 2010, in Rete: <http://www.innovazionepa.gov.it/media/605038/ldo-cda2-v1.0.pdf>.

atto degli interventi del Garante Privacy in tema di FSE, di *dossier* sanitario e di refertazione *on-line* si è sottolineato come questi fosse stato spinto da problemi contingenti a regolare in momenti diversi un fenomeno che, invece, andava affrontato in maniera unitaria, sia per garantire una corretta gestione del dato sanitario in tutte le fasi del suo trattamento, che per permettere al paziente, utente dell'infrastruttura digitale, di esser messo nella condizione di meglio comprendere l'intero sistema, prestando il proprio consenso dopo essere stato informato su tutto il processo informatico in atto.

Si forniranno di seguito alcuni approfondimenti sul tema della refertazione *on-line* alla luce del provvedimento del Garante Privacy, «Linee guida in tema di referti *on-line* – 19 novembre 2009» (LG Referti), nei punti che non sono già stati toccati dalla trattazione che precede.

Il Garante registra l'esistenza di una realtà molto diffusa e caratterizzata dalla messa a disposizione del cittadino della possibilità di accedere al proprio referto medico secondo due modalità: la ricezione dello stesso presso la casella di posta elettronica o il collegamento ad Internet con successivo *download* del documento[104].

Nelle LG Referti si afferma che non consta l'esistenza di una normativa in merito (lo stesso si sostiene a ragione per quanto riguarda i sistemi di FSE) e che, nella quasi totalità delle iniziative esaminate, la refertazione *on-line* non sostituisce le normali procedure (cartacee) di consegna dei referti[105]. A conferma di ciò il Garante cita in nota due disposizioni relative al ritiro dei referti: l'art. 5, comma 8, legge 29 dicembre 1990, n. 407:

[104] Recentissima è la previsione della possibilità per i cittadini di prenotare visite specialistiche, pagare il *ticket* e ritirare referti medici direttamente presso il proprio farmacista: v. Parere del Garante Privacy del 19 febbraio 2011, *Prenotazioni e ritiro analisi in farmacia: via libera del Garante Privacy - 19 gennaio 2011*, in *Boll*., n. 123/gennaio 2011, 0.

[105] LG Referti, p. 1.8.

> Con proprio decreto il Ministro della sanità, sentito il Consiglio superiore di sanità, procede alla revisione del nomenclatore tariffario delle prestazioni specialistiche erogabili a carico del Servizio sanitario nazionale, avuto riguardo alla necessità di individuare le prestazioni tecnologicamente superate nonché quelle il cui costo tariffario risulta eccedente l'onere economico della prestazione stessa e determinando il luogo delle prestazioni genericamente formulate, le singole prestazioni erogabili. Il mancato ritiro del referto entro trenta giorni dall'effettuazione della prestazione specialistica comporta l'addebito all'assistito dell'intero costo della prestazione fruita;

e l'art. 4, co. 18, legge 30 dicembre 1991, n. 412:

> Dal 1° gennaio 1992 i cittadini che non abbiano ritirato i risultati di visite o esami diagnostici e di laboratorio sono tenuti al pagamento per intero della prestazione usufruita. È compito dell'amministratore straordinario della unità sanitaria locale stabilire le modalità più idonee al recupero delle somme dovute.

Questo passaggio non appare pienamente convincente. Il referto diagnostico, infatti, è a tutti gli effetti un documento ai sensi dell'art. 2702 Codice Civile (d'ora in avanti: c.c.) – la norma che disciplina i requisiti di efficacia della scrittura privata – il quale, come noto, consta di due elementi: la dichiarazione scritta proveniente dal soggetto interessato (non necessariamente autografa) e la sottoscrizione di quest'ultimo. Da ciò deriva che si debba considerare sufficiente qualsiasi forma di referto, purché idonea a raggiungere lo scopo desiderato. Con riferimento all'esigenza del pagamento (l'unica dichiarata nelle norme sopra citate), poi, occorre ricordare l'entrata in vigore della previsione di cui all'art. 5 CAD, la quale sancisce l'obbligo per le pubbliche amministrazioni di consentire l'effettuazione di pagamenti ad esse spettanti a qual-

siasi titolo dovuti, con l'uso delle tecnologie dell'informazione e della comunicazione[106].

Il referto, per avere validità giuridica ed acquisire pieno valore legale e probatorio, va sottoposto alla sottoscrizione del medico refertante, il quale con tale operazione assume la responsabilità e la paternità dell'atto. Non riveste alcuna rilevanza chi materialmente ha redatto il testo del referto, bensì chi vi appone in calce la propria sottoscrizione autografa.

Traducendo il tutto in termini informatici: responsabile dell'atto medico non è colui il quale compone, digitandolo, il testo del documento nell'applicativo utilizzato dalla struttura di riferimento, bensì chi appone la propria firma elettronica avanzata al documento informatico nel quale questo testo viene ad essere conchiuso a seguito della sua validazione (artt. 21 e 22 CAD).

Il CAD (richiamato dallo stesso Garante) stabilisce la disciplina rilevante in tema di firme elettroniche. L'art. 35 (Dispositivi sicuri e procedure per la generazione delle firme) indica l'insieme delle procedure e dispositivi coinvolti nelle operazioni di firma (sia *hardware* che *software*), prescrivendo vincoli precisi per il loro utilizzo[107]. Da un pun-

[106] La norma è in attesa di una definizione di dettaglio affidata al Ministero ed alle Regioni o Provincie autonome interessate.

[107] Correttamente il CAD stabilisce vincoli diversificati allorquando si utilizzino procedure automatiche di apposizione della firma. Da un punto di vista procedurale-organizzativo, si ritrovano, infatti, due procedure di firma-validazione dei documenti informatici. Da un lato abbiamo la «firma singola apposta in contesto interattivo», la quale consiste nel classico caso della firma digitale che un utente appone ad uno specifico referto redatto in modalità manuale o quasi manuale: in tale caso si può presumere che l'utente, avendo provveduto personalmente alla costruzione interattiva del contenuto, abbia posto in essere un qualche controllo visivo sul contenuto stesso. Per tale ipotesi, l'art. 35, co. 2, CAD sancisce che: «I documenti informatici devono essere presentati al titolare, prima dell'apposizione della firma, chiaramente e senza ambiguità, e si deve richiedere conferma della volontà di generare la firma». Dall'altro lato, abbiamo il caso delle «firme apposte con procedura automatica»: un sistema di firma automatica viene avviato per processare in modo automatico appunto, un flusso di documenti che il titolare della chiave privata non ha modo di controllare puntualmente. Tale modalità di

to di vista probatorio, il documento informatico sottoscritto con firma elettronica avanzata riveste, dunque, lo stesso forte valore di prova proprio del tradizionale documento analogico sottoscritto di pugno. Anzi, le caratteristiche tecnico-informatiche fanno sì che la prova acquisti un valore ancora più elevato: si presume, infatti, che chi ha apposto una firma elettronica avanzata su un documento informatico sia davvero il titolare del certificato di firma in esso contenuto, determinando così una presunzione giuridica che sarà arduo riuscire a superare (art. 21, co. 2, CAD). Per questi motivi, pur essendo auspicabile un intervento chiarificatore del legislatore per aggiornare una normativa che, con il riferimento all'atto fisico e materiale del «ritiro» dei referti cartacei, denuncia ormai inesorabilmente la sua obsolescenza, occorre rilevare che, in base alla normativa vigente, nulla impedisce in linea di principio di interpretare estensivamente tale «ritiro» facendolo coincidere con l'atto telematico che permette all'interessato di prendere cognizione e di avere la disponibilità di una copia del documento elettronico del referto, opportunamente sottoscritto, come già ricordato, in base al CAD[108].

La facoltatività del servizio di refertazione *on-line* deriva, come abbiamo visto, dalla mancanza di un sostrato normativo che ne disciplini (o comunque ne imponga) l'utilizzo da parte delle strutture sanitarie[109]. Da ciò discendono una serie di conseguenze. I servizi sono, ap-

firma è sicuramente legittima ma va conformata a quando disposto dall'art. 35, co. 3, CAD: «La firma con procedura automatica è valida se apposta previo consenso del titolare all'adozione della procedura medesima». Va ricordato, infine, che l'art. 4, co. 2, del d.p.c.m. 30 marzo 2009, contenente le regole tecniche in materia di firme elettroniche, dispone che «Se il titolare appone la sua firma per mezzo di una procedura automatica, deve utilizzare una coppia di chiavi diversa da tutte le altre in suo possesso»: ciò evidentemente al fine di rendere chiaramente identificabili i documenti firmati attraverso tale procedura automatica.

[108] Con specifico riferimento al referto occorre sottolinearne la piena validità ad ogni effetto di legge, purché la formazione del documento, la sua memorizzazione, conservazione, validazione temporale e la sua trasmissione sia operata nel rispetto delle regole tecniche stabilite dall'art. 71 CAD.

[109] LG Referti, p. 2.2.

punto, facoltativi per l'interessato, il quale deve avere la possibilità di scegliere in piena libertà se accedere o meno al servizio stesso, potendo manifestare una volontà contraria in relazione a singoli esami.

Un punto sicuramente di non agevole applicazione è rappresentato dalla possibilità che l'interessato acconsenta alla comunicazione dei risultati diagnostici al medico curante o al MMG-PLS, dichiarando la sua volontà di volta in volta[110]. Come nel caso dell'accesso al FSE, si pone qui l'esigenza di predisporre un'infrastruttura che renda modulabile la gestione dell'accesso ai referti che riguardano un soggetto, il quale, alla luce del principio di autodeterminazione, dovrebbe esser in grado di avere il pieno controllo dei dati che lo riguardano. L'organizzazione modulare del sistema di refertazione *on-line*, al fine di garantire la possibilità al paziente di scegliere i livelli di comunicazione dei propri referti medici, va necessariamente gestita congiuntamente alla necessità di garantire il diritto all'oscuramento, da parte del paziente stesso, dei dati inseriti nel FSE. Appaiono evidenti le difficoltà che, anche solo sul piano delle economie di scala, si paleserebbero ove si volesse interpretare in via estensiva tale possibilità, richiedendo l'ottenimento di un consenso in forma cartacea per ogni momento decisionale. Si potrebbe, allora, suggerire l'implementazione di un sistema basato su una logica di *opt-in* per quanto concerne il momento iniziale di gestione di questo tipo di trattamento dei dati, completato da una logica di *opt-out* casistica e modulare (e sempre azionabile dal paziente interessato) per ogni circostanza in cui – per qualsiasi motivo percepito come valido dall'interessato – si scegliesse di non ottenere il referto nella modalità online. Una soluzione praticabile può essere quella di un sistema che contempli due tipi di consenso: quello «generale», depositato nell'anagrafica dell'assistito, raccolto ogni volta che si cambia medico curante e quello «di contatto», raccolto in occasione di ogni contatto di cura con l'azienda sanitaria, attraverso il quale gestire le comunicazioni in rela-

[110] *Ibidem*, p. 2.5.

zione allo specifico episodio clinico[111]. Il consenso di contatto, ove presente, prevarrà sul consenso generale. Quando il sistema registra che l'utente non ha espresso alcun tipo di consenso, esso impedisce la comunicazione dei referti in via elettronica dei dati sanitari.

L'informativa, che può anche essere fornita assieme a quella relativa al trattamento dei dati personali, deve comunque evidenziare tutti gli elementi richiesti dall'art. 13 Codice Privacy e descrivere i termini del servizio offerto, sottolineandone la facoltatività[112]. Anche il consenso, sebbene possa esser raccolto contestualmente a quello necessario al trattamento per finalità di cura e prevenzione, deve caratterizzarsi di una propria autonomia e specificità. Risulta evidente l'opportunità di prevedere la raccolta del consenso per questo tipo di servizio contestualmente a quella necessaria per l'implementazione ed il trattamento dei dati attraverso un sistema di FSE. Questa soluzione appare ottimale sotto almeno due punti di vista: sul versante tecnico-organizzativo renderebbe più efficiente l'operare dei soggetti preposti al trattamento dei dati; sul piano dell'utente-paziente garantirebbe una migliore comprensione del processo in atto, permettendogli di comprendere la logica di un intero trattamento dei propri dati sanitari declinato in varie fasi ed applicazioni rispetto ad un trattamento suddiviso in più processi apparentemente, quando non realmente, dissociati gli uni dagli altri.

Con riferimento alla comunicazione dei dati sanitari all'interessato, le LG Referti richiamano l'importanza del rispetto dell'art. 84, di cui *supra* si è approfonditamente trattato[113].

---

[111] Si v. l'esempio dell'Azienda Provinciale per i Servizi Sanitari (APSS) della Provincia autonoma di Trento. Per maggiori informazioni si rimanda al sito web dedicato: <http://www.apss.tn.it/public/ddw.aspx?n=48890>; si v. anche la pagina relativa al servizio aziendale di interconnessione telematica: <http://www.apss.tn.it/public/ddw.aspx?n=49003&h=-2147442770>.

[112] LG Referti, p. 3 «Informativa e consenso».

[113] *Ibidem*, p. 5 «Comunicazione dei dati all'interessato».

Il Garante, poi, registra la possibilità offerta in alcune realtà di archiviare presso la struttura sanitaria tutti i referti prodotti presso i laboratori della stessa[114]. L'archivio è consultabile *on-line* con la possibilità, generalmente, di scaricarne i documenti. Come risulta già chiaro dalla lettura delle LG Referti, il servizio di archiviazione dei referti configura la definizione di *dossier* di cui alle LG FSE. In realtà andrebbe svolta una riflessione – che manca quasi completamente nel panorama italiano – soprattutto con riguardo al tempo ed alle modalità di ritenzione dei referti clinici e dei documenti sanitari in genere. L'esigenza di una conservazione illimitata nel tempo, così come previsto dalla normativa in vigore, va declinata nel nuovo contesto tecnologico che altera e modifica le problematiche (v. problema dell'obsolescenza dei certificati delle firme digitali).

Appare, poi, inopportuna la previsione di garantire la «disponibilità limitata nel tempo del referto *on-line* (massimo 45 giorni)»[115]. La disposizione potrebbe trovare la sua *ratio* nella volontà di garantire un più elevato livello di sicurezza nella gestione dei dati sanitari grazie alla cancellazione del dato stesso; ciò al fine di evitare lo scaricamento da parte di un soggetto non autorizzato. Essa, però, perde qualsiasi ragion d'essere se il sistema di refertazione *on-line* viene concepito nella logica allargata del FSE, per la quale il dato sarà sempre presente nel fascicolo del cittadino, il quale potrà deciderne l'oscuramento nei confronti di determinati professionisti[116].

In chiusura della LG Referti si trovano alcuni riferimenti in ordine alla sicurezza del sistema: a tal proposito il modello che prevede la

[114] *Ibidem*, p. 4 «Archivio dei referti».

[115] *Ibidem*, p. 6.2.

[116] Dobbiamo, infatti, immaginare uno scenario di questo tipo: il paziente scarica il referto attraverso il portale dell'azienda sanitaria dalla stessa applicazione che gli consente la gestione del suo FSE; la possibilità che egli poi disponga di una propria isola di dati dove poter caricare le proprie auto-misurazioni ma anche tutti gli eventi clinici che lo riguardano, rende evidentemente assurda la previsione che i referti che egli può scaricare – e nel caso ricaricare – dalla piattaforma gli siano poi oscurati.

possibilità di scaricare il referto direttamente dal portale dell'azienda sanitaria appare certamente più sicuro di un sistema di spedizione attraverso la posta elettronica, quantomeno fino a che l'uso della posta elettronica certificata non si sarà affermato in maniera significativa anche tra i privati cittadini[117].

[117] LG Referti, p. 6 «Misure di sicurezza e tempi di conservazione dei dati».

CAPITOLO III

ASPETTI NOTEVOLI E NODI PROBLEMATICI

1. Premessa

I sistemi di FSE si connotano per caratteristiche e peculiarità che incidono profondamente sul vivere quotidiano e sul mondo del diritto. A fronte di un nuovo strumento così potente nelle mani sia dei soggetti che erogano servizi sanitari (in generale quindi del SSN), che dei pazienti-utenti i quali possono finalmente partecipare attivamente, e consapevolmente, ai processi curativi che li riguardano, i mutamenti di ordine organizzativo e giuridico sono molteplici: le ASL devono definire nuovi protocolli di gestione dei servizi ed in generale dei flussi informativi; i concetti, le classificazioni e le regole giuridiche tradizionali divengono obsolete. Inoltre, il FSE provoca cambiamenti anche su un piano più prettamente sociale: il secolare, per non dire millenario, rapporto medico-paziente muta le sue caratteristiche, modifica schemi consolidati, altera compiti ed interessi cristallizzati nel tempo.

Per questi e molti altri aspetti, il fenomeno dell'implementazione dei sistemi di FSE diviene un caso paradigmatico al fine di valutare l'impatto delle tecnologie digitali nel contesto giuridico[1]. Si possono, infatti, ritrovare nelle pagine che precedono le medesime problematiche che caratterizzano gli studi che hanno ad oggetto l'analisi dei mutamenti nel campo del diritto apportati più in generale dall'avvento dell'informatizzazione. Il fenomeno più facilmente registrabile, ma di

[1] Sul «diritto dell'era digitale» si v. in generale PASCUZZI, *Il diritto dell'era digitale*, cit.; in particolare si trovano elencate e descritte le caratteristiche ivi in 267-300.

non facile lettura, è quello della dematerializzazione, che investe via via sempre nuovi ambiti dell'agire delle persone: dal commercio elettronico, ai documenti informatici, ai sistemi di pagamento *on-line*. La digitalizzazione della gestione dei dati sanitari porta con se diversi problemi legati ad un passaggio dalla carta al *bit* che appare propagandisticamente imminente nel suo compimento, ma tutt'altro che facile nella sua effettiva realizzazione[2]. Come avremo modo di spiegare meglio più avanti, si determina un cambiamento, per certi versi un sovvertimento, del tradizionale sistema delle fonti, con una sempre più preminente importanza di regole che trovano la loro fonte a livello diffuso, spesso imposte dalla tecnica stessa che diviene così un nuovo formante («formante tecnologico»)[3]. All'affermarsi dell'importanza della tecnica come fonte di regole per il comportamento umano si ricollega un tema centrale nello studio delle norme che disciplinano i fenomeni tecnologici-digitali, quello degli standard[4]. La capacità sovversiva del fenomeno che qui studiamo sul sistema delle fonti ha chiare conseguenze anche all'interno dei complessi di regole che governano gli ambiti dell'agire umano: la disciplina in materia di protezione di dati personali rende palese, soprattutto a livello dei suoi nomenclatori, le difficoltà legate al tentativo di applicare vecchie regole a nuovi fenomeni. Infine, innovative modalità di interazione fanno capolino nel panorama delle relazioni umane. Le tecnologie digitali hanno già dimostrato tale capacità in molti altri contesti (si pensi alla sorprendente fortuna dei sistemi di *social network*): le giornate degli utenti di Internet si colorano di possibilità nuove con riferimento ai livelli di condivisione di idee ed informazioni

[2] Cfr. *idem*, 291-296, in part. 291: «Caratteristica dell'era digitale è la dematerializzazione. I referenti della disciplina giuridica non sono atomi (parti fondamentali della materia e delle cose) ma sequenze di *bit* che rilevano in quanto costitutivi di beni (ad esempio software) o di rapporti (ad esempio lo *streaming* di brani musicali via rete)».

[3] Sulla teoria dei formanti v. R. SACCO, *Formante*, in *Digesto civ*., Torino, 1992, vol. VIII, 438.

[4] V. approfondimenti *supra*.

che possono essere posti in essere nel contesto digitale. Da questo punto di vista, la sanità elettronica non rappresenta che un ulteriore tassello in un contesto sociale sempre più «digitalmente» condizionato.

In questo capitolo si offrirà un approfondimento su alcuni aspetti salienti del FSE all'interno del più generale contesto del diritto dell'era digitale. Si analizzeranno le peculiarità del sistema delle fonti che caratterizza la protezione dei dati personali, cercando di evidenziare novità e paradossi di una disciplina che, pur in origine ideata per essere unitaria, diviene giorno dopo giorno sempre più frammentata tra fonti primarie e secondarie, ponendo in maniera via via pressante il problema del loro coordinamento. Uno spazio *ad hoc* verrà, poi, riservato al tema dell'obsolescenza dei nomenclatori della «vecchia» normativa in materia di protezione dei dati personali: i sistemi di gestione digitalizzata dei dati sanitari mettono in crisi un apparato giuridico concepito per un contesto tecnologico oramai consegnato al passato.

Si focalizzerà, poi, l'attenzione sull'analisi del principio di necessità del trattamento sancito all'art. 3 del Codice Privacy e sul tema delle misure di sicurezza: la garanzia del sistema di tutele concepito all'interno della disciplina in materia di protezione dei dati personali esige l'incorporazione all'interno delle infrastrutture informatiche di principi e valori giuridici, cioè quando la piattaforma viene pensata e costruita. In chiusura di capitolo, si offriranno alcune considerazioni che proiettano nel futuro l'uso di strumenti di gestione informatizzata dei dati sanitari ed ipotizzano nuovi scenari. Un primo paragrafo si concentrerà, pertanto, sulla possibile, prevedibile interazione tra i sistemi di FSE e le biobanche di ricerca, una realtà che si sta progressivamente affermando nel panorama internazionale e nazionale e che risulta di grande interesse per la scienza medica. Un secondo ed ultimo paragrafo, invece, verrà dedicato alle nuove esigenze che vengono presentate dagli utenti dei servizi *on-line* in generale, i quali chiedono che questi ultimi possano essere profilati con grande elasticità applicativa,

per adattarsi al meglio alle caleidoscopiche necessità quotidiane di ciascuno: poter «delegare» l'accesso alla pagina riservata all'interno del portale che ospita ed eroga il servizio rivolto all'utente di un'amministrazione digitale identifica una di queste nuove richieste. Il tema fatalmente si incrocia con gli sviluppi che la sanità elettronica sta conoscendo dal punto di vista della necessità di regolare le relazioni che i vari attori in essa coinvolti (distinguibili, in linea generale, in erogatori e destinatari delle prestazioni sanitarie) tendono sempre più ad instaurare sfruttando le potenzialità concesse dall'avvento del *bit*.

2. Sistema delle fonti del Fascicolo Sanitario Elettronico

I bisogni della società hanno trasformato i computer, inizialmente utilizzati da pochi enti pubblici o da imprese commerciali, in *personal* computer, oramai presenti in tutte le abitazioni. Alle origini, l'elaboratore elettronico rappresentava un nuovo strumento atto a svolgere operazioni di trattamento di dati di carattere militare o attività multifunzione, quali il calcolo, il gioco, la video-scrittura. Più tardi divenne un dispositivo multimediale e globale connesso ad Internet. La Rete stessa si è sviluppata partendo come chiusa, concepita per scopi militari, per poi divenire un sistema aperto di interconnessione universitaria della comunità scientifica, giungendo, infine, negli uffici e nella case di tutti.

Questo fenomeno espansivo e pervasivo delle tecnologie digitali ha determinato il sorgere di processi di deterritorializzazione e destatualizzazione del diritto che hanno fatto arretrare il ruolo del diritto statale sino a spingere verso una rideterminazione del sistema delle fonti delle regole giuridiche[5].

[5] Cfr. PASCUZZI, *Il diritto dell'era digitale*, cit., 297. Sul punto v. anche B.M.J. VAN KLNIK, J.E.J. PRINS, *Law and regulation: scenarios for the information age*, Amster-

La ricerca della disciplina del FSE è caratterizzata da grandi difficoltà ricostruttive. Essa risente delle problematiche comuni nell'analisi delle normative di settore (come ad es. quella in materia di protezione dei dati personali) direttamente interessate dall'incessante e costante mutamento sociale e tecnico. Tecnica che, a fronte di una normativa che appare sempre più diffusa e contenuta in fonti di diversa natura, si afferma a sua volta come possibile fonte di regole per il sistema stesso. Procediamo con ordine, cercando di riassumere brevemente contenuti già presenti nella trattazione che precede al fine di poter svolgere considerazioni di più ampio respiro[6].

A livello di regole generali, la disciplina sulla privacy si ritrova innanzitutto scolpita nelle due direttive di riferimento: Dir. 95/46/Ce e Dir. 2002/58/Ce[7]. Queste sono state recepite in diversi momenti all'interno del nostro ordinamento. La prima regolamentazione in tema di trattamento dei dati personali si è avuta con la l. 675/1996; come noto, ora la fonte di riferimento è rappresentata dal Codice Privacy, il quale rientra, da un punto di vista storico, in una fase regolamentatrice nella quale si è fatto massivo ricorso ai c.d. «codici di settore», con fun-

dam, 2002, 49 ove si legge: «the growth of information and communication technology is having drastic consequences for familiar notions seem to points of departure of our legal system. Some legal notions seem to lose their validity entirely or partially in a digital environment» e più avanti «the question is therefore whether the national government still has a role to play at all in the regulation of electronic communication».

[6] Uno studio ricostruttivo delle fonti normative in materia di protezione di dati personali si trova in N. LUPO, *Le fonti normative della privacy*, *tra esigenze di aggiornamento e ricerca di stabilità*, in CUFFARO, D'ORAZIO, RICCIUTO (a cura di), *Il codice del trattamento dei dati personali*, cit., 777-810. La tematica può anche essere affrontata dal punto di vista dei cambiamenti che stanno investendo il diritto privato sempre più condizionato dal rapporto tra fonti statali e legislazione regionale: per approfondimenti v. A.M. BENEDETTI, *L'autonomia privata di fronte "diritto privato delle regioni"*. Corte cost. sent., 13 novembre 2009, n. 295, in *Contratti*, 2010, 113; N. LIPARI, *Il diritto privato tra fonti statali e legislazione regionale*, in *Giur. it*., 2003, 3; V. ROPPO, *Diritto privato regionale?*, in *Riv. dir. priv*., 2003, 11. Più in generale, sulla crisi del sistema delle fonti nel diritto civile, v. N. LIPARI, *Le fonti del diritto*, Milano, 2008.

[7] Così come modificata dalla Dir. 2009/136/Ce.

zione di coordinamento, riassetto e semplificazione della disciplina di materie determinate, e con evidenti spinte verso l'innovazione della stessa. Con questo intervento normativo, infatti, il nostro legislatore ha inteso riorganizzare e sistematizzare l'impianto regolamentativo della protezione dei dati personali prima sparso in atti provenienti da diverse fonti[8]. In particolare, per quanto qui interessa, al trattamento dei dati personali in ambito sanitario è dedicato il Titolo V del Codice (artt. 75-94).

Come è stato già ricordato, non esiste a livello di fonte primaria una normativa *ad hoc* in tema di FSE: le difficoltà che tale mancanza determina sono di tutta evidenza[9]. Nel silenzio del legislatore, è inter-

[8] Cfr. V. SCALISI, *Complessità e sistema delle fonti di diritto privato*, in *Riv. dir. civ*., 2009, 147, ove vengono sapientemente analizzate e tratteggiate le caratteristiche proprie del sistema delle fonti di diritto privato nello svolgersi delle fasi prima assolutizzanti ed unificatrici e, poi, disgreganti e più aderenti alla complessità del fenomeno giuridico. Sul punto del rapporto tra i codici di settore ed il Codice Civile v. in part. 155: «Considerati come il *compimento* della codificazione in realtà tali codici, almeno per i profili regolai, svuotano ed esautorano il codice: ciò nonostante – a meno di non raccogliere e dare attuazione a normative di derivazione comunitaria – neppure essi, al pari delle leggi decodificanti, creano verticalizzazione e quindi disposizione gerarchica delle rispettive normative, in quanto operanti su un piano parallelo e orizzontale *accanto* al codice civile, con il quale interagiscono in termini se mai di eventuali deroghe o abrogazione tacita per incompatibilità».

[9] È stato presentato in data 16 luglio 2010 dal Ministro della Salute Ferruccio Fazio uno schema di disegno di legge recante «Sperimentazione clinica e altre disposizioni sanitarie», riguardante la sperimentazione clinica, appunto, la riforma degli ordini professionali dei medici, i dispositivi medici e altre norme di interesse sanitario, il quale all'art. 15, rubricato «Disposizioni in materia di fascicolo sanitario elettronico», conteneva i primi riferimenti utili alla definizione normativa del FSE. Il d.d.l. aveva ricevuto una prima approvazione da parte del Governo nella riunione del Consiglio dei Ministri del 24 settembre 2010. Successivamente esso era stato sottoposto e aveva ottenuto il parere favorevole dalla Conferenza Stato-regioni (il testo del parere è reperibile in Rete: <http://www.governo.it/GovernoInforma/Dossier/professioni_sanitarie/parere_regioni28102010.pdf>). Il d.d.l. «Delega al Governo per il riassetto della normativa in materia di sperimentazione clinica e per la riforma degli ordini delle professioni sanitarie, nonché disposizioni in materia sanitaria» è stato, da ultimo, approvato in via definitiva dal Consiglio dei Ministri in data 10 marzo 2011 (in Rete

venuto il Garante Privacy con due provvedimenti a carattere generale: LG FSE del 16 luglio 2009 e LG Referti del 19 novembre 2009, già ampiamente ricostruiti e commentati nel secondo capitolo della presente opera. Questi erano stati preceduti a livello europeo da un documento di orientamento privo di valore vincolante, il già citato Documento CCE Gruppo art. 29 del 15 febbraio 2007.

Occorre, allora, interrogarsi su quali siano le tendenze in atto con riferimento al sistema delle fonti del diritto, allorché quella che appariva essere un'istanza semplificatrice e razionalizzatrice – ci si riferisce ai tentativi di sistematizzare all'interno di testi unici la disciplina di materie di settore – in realtà presenta problematiche e complessità determinate dalla diffusione dell'azione del legislatore e dall'intervento di nuovi attori sul versante della creazione di norme e regole[10]. La disciplina sulla protezione dei dati personali rappresenta, infatti, un caso emblematico delle recenti dinamiche di trasformazione del sistema delle fonti del diritto, poiché si ritrovano in essa le principali tendenze in atto sia a livello nazionale che internazionale[11]. Di seguito per punti gli aspetti più rilevanti.

<http://www.governo.it/GovernoInforma/Dossier/professioni_sanitarie/schemaddl.pdf>).

[10] Cfr. SCALISI, *Complessità e sistema delle fonti di diritto privato*, cit., 150: «la complessità dei rapporti e delle relazioni di vita dei consociati avrebbe quanto prima recuperato il terreno perduto sul piano stesso della strutturazione della giuridicità e anzi avrebbe finito con il tradursi in complessità dello stesso intero universo giuridico, in un processo continuo e senza sosta che l'avrebbe portata a trasferirsi negli stessi luoghi della produzione normativa, per influenzare direttamente meccanismi e procedure e dar vita così al proliferare di una varia, complessa e articolata moltitudine di nuove e ulteriori fonti regolative».

[11] Una periodizzazione dei momenti evolutivi della legislazione in materia di privacy si ritrova in LUPO, *Le fonti normative della privacy, tra esigenze di aggiornamento e ricerca di stabilità*, cit., 807-810, ove si richiama sul punto CONFERENZA DEI PRESIDENTI DEI PARLAMENTI ALL'UNIONE EUROPEA, *Complessità normativa e ruolo dei Parlamenti nell'epoca della globalizzazione*, Lisbona, maggio 1999, reperibile in U. DE SIERVO (a cura di), *Osservatorio sulle fonti 1999*, Torino, 1999, 302 ss.; v. anche M. CARTABIA, *Le norme sulla privacy come osservatorio sulle tendenze attuali delle fonti*

Anzitutto, il momento ispirativo della previsione di una normativa *ad hoc* in materia di privacy è stato fortemente influenzato dall'evoluzione dei mercati aperti a livello mondiale, e, più in generale, dal fenomeno della globalizzazione: la legislazione italiana nasce proprio dalla necessità per il nostro Paese di conformarsi ai requisiti necessari per aderire al sistema informativo di Schengen. Tutto ciò con lo scopo di favorire la circolazione delle persone e delle merci[12]. Quindi, l'idea stessa di una normativa sul punto è da considerarsi esogena rispetto al nostro ordinamento.

Inoltre, la prima legge italiana in materia di protezione dei dati personali, la n. 675/1996, rappresenta null'altro che il recepimento della sopra citata Dir. 95/46/Ce. Lo stesso Codice Privacy, pur animato da una volontà di sistematizzazione della disciplina, coincide con il recepimento della Dir. 2002/58/Ce. L'esigenza di fondo è, pertanto, rappresentata dalla necessità di integrazione con ordinamenti diversi. Non solo, dunque, la ragione di una normativa specifica si ritrova al di fuori del nostro sistema, ma anche la sua stessa disciplina è dettata da fonti esterne ad esso[13].

Un terzo aspetto da tenere in considerazione è quello legato allo sviluppo tecnologico, il quale obbliga il diritto ad una continua rincorsa volta a regolamentare fenomeni nuovi e sempre più estesi. Non si può, infatti, dimenticare il ruolo che le regole tecniche, ideate e create da parte di organismi (i c.d. enti di normalizzazione) spesso a carattere privato, stanno assumendo nel contesto digitale. Lo standard tecnico può, infatti, essere considerato sia come una regola che soggiace

---

del diritto, in M.G. LOSANO (a cura di), *La legge italiana sulla privacy. Un bilancio dei primi cinque anni*, Roma – Bari, 2001, 61 ss.

[12] LUPO, *Le fonti normative della privacy, tra esigenze di aggiornamento e ricerca di stabilità*, cit., 807.

[13] *Ibidem*, 807-808. Si assiste ad una «progressiva "secondarizzazione" delle norme primarie dell'ordinamento interno»: in A. SIMONCINI, *Il sistema delle fonti normative*, in V. CUFFARO, V. RICCIUTO (a cura di), *Il trattamento dei dati personali. Vol. II: profili applicativi*, Torino, 1999, 11, 18.

all'azione del diritto statale sia come una norma che, di fatto, prevale sugli ordinamenti territoriali. Quest'ultima sembra la visuale più difficile e, al tempo stesso, maggiormente stimolante, volta a corroborare, con l'esempio delle misure di sicurezza poste a difesa del trattamento informatico dei dati personali, la tesi che addita la tecnica (ed i suoi standard) come una delle fonti più rilevanti (ed aggressive) del diritto dell'era digitale[14].

Nel contesto della protezione dei dati personali viene, poi, attribuito ampio rilievo ai codici deontologici e di buona condotta, i quali vengono configurati in maniera molto simile a fonti del diritto: la loro adozione è, infatti, talvolta obbligatoria e la disciplina in essi prevista è applicabile anche a soggetti diversi da quelli contenuti nella categoria che li ha definiti[15].

---

[14] Più in generale, sulla questione del rapporto tra il «codice», inteso come codice binario, ed il sistema delle fonti del diritto si confrontano diverse opinioni. Da un lato, vi sono coloro che, rimanendo su posizioni più tradizionali e positiviste, non riconoscono valore di «fonte del diritto» al «codice»: cfr. DOMMERING, *Regulating Technology: Code is Not Law*, cit., 11 ss. (l'autore sostiene che il «codice» rappresenta «una mano del diritto»); J.R. REIDENBERG, *'Lex Informatica', The Formulation of Information Policy Rules Through Technology*, 76 *Tech. L. Rev*. 553 (1998), il quale sostiene che la regolamentazione giuridica (*Legal Regulation*) e la *Lex Informatica* rappresentino due distinti strumenti: il primo è *law* ed è volto a disciplinare il territorio fisico, il secondo è definito *architectural standards* ed è concepito per la Rete. Dall'altro lato, vi sono coloro che sono propensi a considerare il codice come una vera e propria fonte del diritto: v., tra tutti, LESSIG, *Open Code and Open Societies*, cit., *passim*; ID., *Code and Other Laws of Cyberspace*, cit., *passim*. Analizzando la questione con mente aperta, dobbiamo riconoscere che il codice influenza i comportamenti degli individui e quindi, almeno dal punto di vista dei suoi effetti, funziona come una regola giuridica. Compreso ciò, è di tutta evidenza l'importanza che l'ordinamento si occupi anche di questo settore, quanto meno per contribuirne alla regolamentazione. Tale tesi si basa sull'assunto che la caratteristica essenziale delle fonti del diritto sia quella di condizionare il comportamento umano (punto di vista caro ai comparatisti): se è così, allora non si può negare al codice un posto nel sistema delle fonti. Per maggiori approfondimenti sul rapporto tra architetture digitali e diritto v. A. ROSSATO, *Diritto e architettura nello spazio digitale: il ruolo del software libero*, Padova, 2006.

[15] Cfr. LUPO, *Le fonti normative della privacy, tra esigenze di aggiornamento e ricerca di stabilità*, cit., 809 ed i riferimenti ivi contenuti.

L'aspetto sicuramente più interessante, e sul quale è opportuno concentrare la nostra attenzione, è quello collegato all'attività regolamentare posta in essere dalle autorità indipendenti; ciò è dovuto all'elevato tasso di complessità tecnica legato alla molteplicità degli interventi tra loro collegati i quali richiedono un alto grado di coerenza e, soprattutto, di efficacia per raggiungere i risultati finali desiderati[16]. Il Garante Privacy riveste un ruolo di primo attore nell'attività di vigilanza e, soprattutto, di indirizzo con riferimento all'adozione e rispetto della disciplina in materia di protezione dei dati personali[17]. Anzi esso si comporta spesso quasi come una sorta di «legislatore supplente» laddove quello vero e proprio non sia intervenuto ad aggiornare-profilare la disciplina di cui al Codice al mutato contesto tecnologico e sociale. Lo strumento utilizzato è quello dei provvedimenti a carattere generale che contengono linee guida rivolte agli operatori del settore. Questo, come abbiamo visto, è quanto accaduto in materia di FSE.

Occorre allora interrogarsi su quale sia il reale valore cogente di questi atti che, pur promanando da un'autorità indipendente, di fatto divengono l'unico o il prevalente punto di riferimento normativo. Le LG FSE e le LG Referti sono state emanate dal Garante Privacy ai sensi dell'art. 154, co. 1, lett. h, il quale recita:

> Oltre a quanto previsto da specifiche disposizioni, il Garante, anche avvalendosi dell'ufficio e in conformità al presente codice, ha il compito di: […] curare la conoscenza tra il pubblico della disciplina rilevante in materia di trattamento dei dati personali e delle relative finalità, nonché delle misure di sicurezza dei dati[18].

---

[16] *Ibidem*, 809-810.

[17] Il Garante Privacy è stato istituito dalla l. 675/1996 in conformità alla Dir. 95/46/Ce, la quale all'art. 28 richiedeva esplicitamente a ciascun Stato membro di prevedere uno o più autorità di controllo che fossero «pienamente indipendenti nell'esercizio delle funzioni loro attribuite».

[18] Per approfondimenti v. BIANCA, BUSNELLI (a cura di), *La protezione dei dati personali*, cit., art. 154, 1978, 1989 (commento DI C. LACAVA, L. CERRONI).

Questa funzione amplifica l'importanza culturale del fenomeno: per favorire l'osservanza delle norme nel tempo e per permettere al singolo di conseguire una piena consapevolezza dell'ambito di protezione dei propri dati personali occorre formare una coscienza collettiva sul tema della privacy. Il problema sorge però se, come statuito da una recente sentenza di merito, non si riconosce a tali interventi del Garante alcun contenuto cogente[19]. L'oggetto del contendere verteva in realtà sul valore delle «Linee guida in materia di trattamento di dati personali da parte dei consulenti tecnici e dei periti ausiliari del giudice e del pubblico ministero» adottate in data 31 luglio 2008. Ebbene, il giudice di primo grado ha negato tale valore, in quanto

> il provvedimento impugnato, in ogni caso, risulta privo di alcun contenuto precettivo immediato, costituendo di tutta evidenza mero strumento interpretativo non vincolante[20].

L'unico effetto che giuridicamente viene riconosciuto alle suddette LG è quello

> meramente indiretto di costituire una garanzia privilegiata di corretto trattamento dei dati personali ad opera dei consulenti dell'Autorità giudiziaria che, nella loro attività di analisi e valutazione dei dati stessi, vi si uniformino[21].

La questione è complessa e di non facile soluzione. Nel silenzio del legislatore, rimangono le difficoltà pratiche di coloro i quali sono chiamati a cimentarsi con l'adozione dei sistemi di FSE. A questi l'amletico dubbio: seguire le LG che il Garante propone e conformarsi alla sua, autorevole, lettura dei principi del Codice Privacy (ricevendo,

[19] Cfr. Trib. Bassano del Grappa, 12 maggio 2009, inedita, in Rete: <http://www.aipros.org/oldsite/Documenti/Riservato/SentenzaBassano.pdf>.

[20] *Ibidem*.

[21] *Ibidem*.

tramite le sue indicazioni, una sorta di certificazione della bontà del modello che si intende implementare), ovvero scegliere la via perigliosa della propria interpretazione, accettando la possibilità di assumersi in proprio l'esclusiva responsabilità, qualora si venga infine chiamati a rispondere di una qualche violazione?

3. Obsolescenza della struttura e dei nomenclatori propri della normativa in materia di protezione dei dati personali

Come si è appena constatato, la regolamentazione della tutela dei dati personali ha risentito di spinte, condizionamenti e mutamenti in larga parte mossi da fenomeni che investono l'intero ordinamento giuridico. Le regole volte a governare l'utilizzo delle nuove tecnologie, ed in special misura quelle collegate alle tecnologie digitali, risentono di influenze ancor più forti, dovute al rapidissimo ed incessante evolvere del progresso scientifico che le rende presto obsolete[22]. Verrebbe da esclamare «Sed fugit interea fugit irreparabile tempus»[23].

Ciò è avvenuto anche nell'ambito della normativa sulla privacy, con riferimento sia alla struttura dell'impianto regolamentativo, che alle stesse tassonomie atte a descrivere soggetti ed oggetti del sistema. La sanità elettronica, ed in particolare l'esperienza in via di affermazione dei sistemi di FSE, non hanno fatto altro che palesare ancora più tale scollamento tra realtà e norme giuridiche: il ripensare regole e prassi organizzative alla luce della nuova esigenza di gestire digitalmente i dati sanitari – all'interno di architetture che garantiscano elevatissimi livelli di sicurezza e riservatezza dei dati, riconoscendo, al tempo stesso, al paziente un ruolo (informativo) centrale – rende evidenti le difficoltà

[22] Cfr. PASCUZZI, *Il diritto dell'era digitale*, cit., 311: «Se le regole sono in qualche modo "figlie" delle tecnologie, occorrerebbe evitare di applicare meccanicamente a nuove tecnologie regole nate come proiezioni di altre tecnologie».

[23] VIRGILIO, *Georgiche*, Libro terzo.

attuative di un Codice Privacy pensato per un contesto tecnologico almeno in parte relegato nel passato.

La Dir. 95/46/Ce interveniva in un ben determinato momento storico. I *personal computer* si erano via via diffusi nel tessuto sociale dei vari Paesi europei, i quali avevano cominciato a dotarsi di una normativa di settore atta a gestire il fenomeno del trattamento dei dati in maniera informatizzata (l'Italia fu la penultima in Europa a prevedere una disciplina *ad hoc* in materia). L'esigenza più sentita da parte delle istituzioni europee era allora quella di dar vita ad un efficiente mercato unico, il quale veniva evidentemente ostacolato da un intervento in ordine sparso da parte dei diversi Stati sul punto del trattamento dei dati personali: ciò rendeva, di conseguenza, oltremodo difficile la circolazione di beni e servizi e dei lavoratori all'interno della Comunità. La «direttiva madre» in tema di protezione dei dati personali è animata fin dall'inizio dalla volontà di colmare questa disarmonia normativa e di fornire una cornice di riferimento per le legislazioni dei vari Paesi membri. Il contesto tecnologico che fotografa è alquanto particolare: cominciavano a crearsi le prime estese banche dati gestite soprattutto da uffici statali ed imprese private. L'idea di base era quella di proteggerle come fossero «castelli del trattamento» costruendo tutto intorno un sistema di misure di sicurezza volto, da un lato, ad impedire accessi dall'esterno, e, dall'altro, a regolare all'interno i livelli di responsabilità con riferimento ai dati stessi (da qui la gerarchia degli attori del trattamento: titolare, responsabile, incaricato). L'interconnessione tra le varie banche dati, o quantomeno una comunicazione strutturata e costante tra esse, non si era ancora affermata a tal punto da richiedere un'attenta riflessione sulle problematiche che ne potessero derivare. Il ruolo dell'individuo all'interno di tale assetto era del tutto marginale ed a lui veniva riconosciuto il semplice *status* di «interessato al trattamento»,

spettatore qualificato dell'attività che altri ponevano in essere ed avente ad oggetto i suoi dati[24].

Il fenomeno Internet cominciava ad affermarsi nel torno di quegli anni; esso non fu analizzato ed inserito all'interno della cornice di principi stabilita dalla direttiva del 1995. Il mutamento che stava determinando non poteva, però, essere del tutto ignorato; si cominciò pertanto a prendere in considerazione l'opportunità di prevedere una direttiva *ad hoc* con riferimento al trattamento dei dati personali nel contesto delle comunicazioni elettroniche. La riflessione durò sette anni ed esitò, dapprima, nell'emanazione della Dir. 97/66/Ce sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni, per poi essere ripresa ed approdare al secondo provvedimento rappresentato dalla Dir. 2002/58/Ce: questa andava ad abrogare la disciplina del 1997 e cercava di colmare la lacuna normativa e di fornire regole che disciplinassero il trattamento dei dati che avveniva per il tramite di flussi di informazioni che viaggiavano attraverso le reti di comunicazione ed, in particolare, la rete Internet[25]. Assunti, idee di base, categorie si riferivano al contesto tecnologico di fine anni novanta. La comunicazione tra banche dati era sporadica, non ancora strutturata, sicuramente non organizzata in un sistema[26].

Torniamo al caso specifico dei sistemi di FSE. Essi sono caratterizzati dall'interconnessione logica tra banche dati. Non abbiamo, infatti, a che fare con singoli *repository* da proteggere e gestire secondo modalità oramai consolidate nella pratica e che hanno trovato anche espressione nei riferimenti normativi sopra individuati. Ci troviamo di

[24] Come detto la direttiva ha trovato recepimento nell'ordinamento italiano ad opera della l. 675/1996.

[25] Come modificata dalla Dir. 2009/136/Ce.

[26] I Paesi europei hanno provveduto secondo diverse modalità a recepire questa seconda direttiva. L'Italia scelse di rinnovare e sistematizzare la normativa in materia di protezione dei dati personali emanando un nuovo Codice Privacy e recependo la disciplina relativa alle comunicazioni elettroniche all'interno di un apposito Titolo (X).

fronte ad un sistema che sfuma il ruolo del singolo contenitore di dati, e di conseguenza del singolo titolare del trattamento di quest'ultimi, e che esaspera, invece, quello della capacità e potenzialità che il collegamento stabile, coordinato e debitamente gestito tra questi centri di informazioni determina. I flussi di dati diventano il fenomeno più frequente; la gestione da parte di più soggetti assume i caratteri della quotidianità; l'aumento esponenziale dei rischi che incombono sui dati – diretta conseguenza di tutto ciò – emerge come l'aspetto più problematico. Subito ci si rende conto che il castello costruito dall'apparato regolamentativo apprestato dal legislatore europeo e recepito dai diversi legislatori nazionali appare del tutto inadatto a gestire questo nuovo genere di questioni. Ciò essenzialmente su tre fronti. Innanzitutto, il sistema di sicurezza approntato: le misure previste dalla normativa in materia di privacy risultano più congeniali alla protezione di banche dati isolate e non collegate tra loro, quando oramai la partita si gioca sui flussi di informazioni che navigano sulla Rete e che rispondono a relazioni digitalmente instaurate tra i vari recipienti di dati (sistema informativo dell'ospedale, scheda del MMG o del PLS, banca dati del laboratorio di analisi, ecc.). In tale ambito, il sistema di autenticazione e di gestione degli accessi che prima doveva semplicemente fotografare l'attività nel contesto digitale dei vari responsabili ed incaricati del trattamento, i quali all'interno della struttura del titolare provvedevano a trattare i dati secondo le direttive di quest'ultimo, è ora oberato dalla gestione di richieste d'accesso provenienti da soggetti appartenenti a varie strutture, con privilegi connessi ai dati diversificati a seconda dello *status* che essi ricoprono all'interno del complessivo sistema (non hanno più accesso al dato solo il medico o la struttura che l'ha prodotto ma potenzialmente tutti i soggetti che fanno parte dell'intero sistema di FSE, compreso, e non ultimo, il paziente a cui i dati si riferiscono). Inoltre, ad andare in crisi sono anche le tradizionali categorie degli attori della privacy: non essendoci più una singola banca dati da proteggere ed organizzare, il

ruolo di un unico titolare si perde e si va sempre più affermando un'attività di trattamento dei dati comune, anche a livello di responsabilità, a più soggetti. Si comincia, pertanto, a cercare di dare significato ad una locuzione che fino ad oggi era presente tra le categorie utilizzate dal Codice e dalla dottrina ma ancora in cerca di un contenuto normativo-operazionale: la c.d. co-titolarità. Infine, l'impatto è rilevante sulla tassonomia della disciplina sulla privacy, specialmente per quanto riguarda il ruolo da protagonista che viene riconosciuto al paziente all'interno del FSE: l'utente-paziente del sistema acquisisce, grazie a questi nuovi strumenti, capacità che il precedente contesto tecnologico non gli riconoscevano. Questi non è più mero spettatore (dotato certo di diritti di controllo, quali quelli previsti all'art. 7 Codice Privacy) del trattamento posto in essere da altri. Il sistema sempre più si profila e si disegna sul paziente e sulle sue esigenze. Tassello dopo tassello la rivoluzione informatica gli consegna la possibilità di gestire direttamente i suoi dati, fino a permettergli di alimentare personalmente la base informativa in possesso ai soggetti che legittimamente devono prendersi cura della sua salute. Va, quindi, ripensata la categoria di «interessato al trattamento», specialmente in quanto sembra richiamare l'immagine di un semplice ruolo passivo. Il mutato approccio che caratterizza il suo accesso al trattamento dei dati, gestito sì da altri ma ora, in parte, direttamente controllato dal medesimo paziente, dovrebbe poter avere come conseguenza un ripensamento dei nomenclatori usati per definire i ruoli all'interno della struttura che tratta i dati e che costituisce il «cerchio della fiducia» intorno ad essi (più avanti si avrà modo di tornare sul punto con riferimento alla possibilità di delegare l'accesso ai servizi forniti dal proprio FSE da parte del paziente-interessato).

La sanità elettronica può diventare, dunque, l'ambito privilegiato per iniziare a riflettere su un ripensamento, critico, dell'approccio che contraddistingue la nostra disciplina sulla privacy. Il FSE necessita

di un intervento diretto da parte del legislatore volto a sciogliere finalmente nodi e criticità sulla base di una nuova sistematica.

4. Principio di necessità e misure di sicurezza

Sono stati evidenziati nel primo capitolo gli aspetti concettuali e definitori legati al tema della sicurezza informatica. Nel corso del secondo capitolo è stato, poi, dedicato spazio alle questioni più prettamente connesse al trattamento informatizzato dei dati sanitari all'interno dei sistemi di FSE. Si svolgeranno qui alcune brevi considerazioni con riferimento all'importanza che la sicurezza deve rivestire nel contesto del rapporto tra diritto ed informatica, e più in particolare, della programmazione delle piattaforme atte a gestire dati personali e sensibili.

Il Codice Privacy, come sopra ricordato, riserva il Titolo V alla disciplina della «Sicurezza dei dati e dei sistemi», dedicando il Capo I agli obblighi di sicurezza in generale ed il Capo II alle misure minime di sicurezza[27]. La disciplina è contenuta negli articoli 31 e seguenti del Codice e nel suo «Disciplinare tecnico in materia di misure minime di

[27] Sul tema delle misure di sicurezza in materia di privacy, v. C. RABAZZI, P. PERRI, G. ZICCARDI, *La sicurezza informatica e la Privacy*, in G. ZICCARDI (a cura di), *Telematica giuridica. Utilizzo avanzato delle nuove tecnologie da parte del professionista del diritto*, Milano, 2005, 516 ss.; P. PERRI, *Le misure di sicurezza*, in J. MONDUCCI, G. SARTOR, *Il codice in materia di protezione dei dati personali*, cit., 137; A. BIASIOTTI, *Codice della privacy e misure minime di sicurezza: d.lgs. 196/2003*, 2ed., Roma, 2004; G. CORASANITI, *La sicurezza dei dati personali*, in CARDARELLI, SICA, ZENO-ZENCOVICH (a cura di), *Il codice dei dati personali*, cit., 112-163; ID., *Esperienza giuridica e sicurezza informatica*, Milano, 2003, 153-257; F. BERGHELLA, *Guida pratica alle nuove misure di sicurezza per la privacy*, Roma, 2003, 141; P. PERRI, *Introduzione alla sicurezza informatica e giuridica*, in E. PATTARO (a cura di), *Manuale di diritto dell'informatica e delle nuove tecnologie*, Bologna, 2002, 306; M. MAGLIO, *Le misure di sicurezza nei sistemi informativi: il punto di vista di un giurista alla luce della legge sulla tutela informatica*, in *Contratto e imp*., 2000, 1.

sicurezza» (allegato B) [28]. Come criterio più ampio si pone, inoltre, quello sancito all'art. 3, il quale merita, soprattutto, attenzione in quanto rappresenta uno tra gli aspetti più innovativi del Codice Privacy. Esso sancisce, infatti, l'esistenza, all'interno della nostra disciplina sulla protezione dei dati personali, del «principio di necessità nel trattamento dei dati»:

> I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità[29].

[28] L'art. 36 del Codice stabilisce che il Disciplinare Tecnico venga periodicamente aggiornato con decreto del Ministro della giustizia di concerto con il Ministro per le innovazioni e le tecnologie in relazione all'evoluzione tecnica ed all'esperienza maturata nel settore. Il fatto che si preveda la necessità di un aggiornamento costante risponde alle nuove logiche normative in settori in cui la tecnologia gioca un ruolo di rilevante importanza. Si hanno così regolamentazioni a due livelli: un primo livello che stabilisce le regole generali ed i principi di base relativi all'attività che si deve svolgere; un secondo che determina più nel dettaglio gli specifici standard da adottare e che, vista la costante evoluzione tecnologica, sono soggetti ad un necessario, periodico aggiornamento. La disciplina della sicurezza dei dati personali ha ricevuto una riorganizzazione che dovrebbe garantire alla materia quantomeno maggiore sistematicità. Tale intervento, da un lato, sembra mantenere una coerenza complessiva nell'ambito delle previsioni già in vigore, dall'altro definisce l'ambito delle misure, generali e «minime», che devono garantire la sicurezza, nel quale le prescrizioni legislative assumono un ruolo direttamente prescrittivo. La nuova disciplina organizza e salda con maggiore coerenza i precetti sostanziali che erano già rinvenibili nel complesso delle disposizioni previdenti: art. 15, commi 1 e 2, l. 675/1996 ed art. 2 d.lgs. 13 maggio 1998, n. 171.

[29] Sul principio di necessità in dottrina, v. R. D'ORAZIO, *Il principio di necessità nel trattamento dei dati personali*, in CUFFARO, D'ORAZIO, RICCIUTO (a cura di), *Il codice del trattamento dei dati personali*, cit., 20-27; G. RESTA, *Il diritto alla protezione dei dati personali*, in CARDARELLI, SICA, ZENO-ZENCOVICH (a cura di), *Il codice dei dati personali. Temi e problemi*, cit., 45 ss.; A. PALMIERI, R. PARDOLESI, *Il codice in materia di protezione dei dati personali e l'intangibilità della «privacy» comunitaria*. Nota a sent. Corte di Giustizia delle Comunità Europee 6 novembre 2003, n. causa C-101/01, in *Foro it.*, 2004, IV, 59. Un approccio analogo al principio sancito dall'art. 3 Codice

La particolare rilevanza attribuita a questa previsione attraverso la sua collocazione «topografica» all'interno del Codice tra i principi generali si può far derivare dall'opportunità, avvertita con considerevole urgenza dal nostro legislatore, di predisporre idonee forme di tutela per limitare al massimo la circolazione di dati personali connessa all'informatizzazione della società moderna, con specifico riferimento all'esponenziale diffusione dell'utilizzo della Rete.

L'ambito d'applicazione dell'articolo in oggetto è da rinvenirsi in riferimento al trattamento di dati effettuato attraverso l'impiego di «sistemi informativi» e «programmi informatici»[30].

Il principio di necessità rappresenta, in un certo senso, un'anticipazione degli adempimenti previsti dal Titolo V ed impone al titolare del trattamento di adottare delle misure organizzative informatiche idonee ad escludere per quanto possibile l'utilizzo di dati personali ed identificativi. Questo risultato potrà essere perseguito utilizzando dati anonimi o modalità che permettano di identificare l'interessato solo in caso di necessità. Nel primo caso, ci troviamo di fronte ad una specificazione del principio di finalità sancito all'art. 11, comma 1, lett. d, laddove si stabilisce, tra l'altro, che i dati trattati devono essere

> non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati[31].

Privacy è stato adottato dalla Raccomandazione della Commissione europea 2009/387/Ce del 12 maggio 2009 sull'applicazione dei principi di protezione della vita privata e dei dati personali nelle applicazioni basate sull'identificazione a radiofrequenze (tecnologia Rfid), ove si richiama il principio della «sicurezza e tutela della vita privata fin dalla fase di progettazione» (in Rete: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:122:0047:0051:IT:PDF>).

[30] Nel linguaggio corrente l'espressione «sistema informativo» richiama un complesso di risorse (sia di tipo *hardware* che di tipo *software*) finalizzato al trattamento automatizzato delle informazioni; mentre con quella di «programmi informatici» si è semplicemente fornita una traduzione concettuale, anche se non letterale, del termine inglese *software*.

Sul piano dell'attuazione, questa disposizione richiede qualcosa di nuovo e di alquanto oneroso. Essa presuppone cospicui investimenti, tanto sotto il profilo delle risorse informatiche (risultando chiaramente necessario un ripensamento dei sistemi informativi), quanto sotto quello delle risorse umane[32]. La dottrina ha, finora, proposto una lettura riduttiva dell'articolo in oggetto individuando in esso unicamente un criterio di organizzazione tecnica degli archivi informatici finalizzato ad incentivare l'adozione di tecnologie atte a preservare la privacy degli utenti (ad es., le c.d. *privacy enhancing technology* o PET)[33].

---

[31] Quando le finalità per cui i dati sono sottoposti a trattamento possono essere conseguite anche attraverso il trattamento di dati non associabili ad un soggetto identificato, allora il titolare non sarà legittimato ad elaborare dati eccedenti, tra cui sicuramente vanno fatti rientrare quelli relativi all'identificazione dell'interessato. Nel caso, invece, dell'utilizzazione di modalità che permettano di identificare l'interessato solo in caso di necessità, occorre intendere tale previsione come un esplicito riconoscimento di favore legislativo per i trattamenti effettuati attraverso pseudonimi, ovvero scorporando le informazioni trattate in modo tale che l'incaricato non abbia alcuna possibilità di identificare l'interessato cui i dati si riferiscono. L'attività svolta attraverso l'utilizzo di pseudonimi sarà, comunque, soggetta alla disciplina del Codice in quanto l'interessato, seppur indirettamente, potrà essere identificato. Il trattamento sarà, invece, sottratto al Testo Unico nel caso in cui lo pseudonimo stesso sia gestito direttamente ed esclusivamente dall'interessato ed il titolare non abbia alcuna possibilità di associarlo ad un determinato soggetto individuato o individuabile. L'opportunità di incentivare l'utilizzo di pseudonimi è stata, da ultimo, affermata dal Gruppo art. 29 il quale, nella «Raccomandazione relativa ai requisiti minimi per la raccolta di dati *on-line* nell'Unione europea», adottata il 17 maggio 2001, ha suggerito «l'utilizzo di pseudonimi di qualsivoglia natura» per la consultazione in modalità anonima di siti commerciali «qualora sia necessario un collegamento ad una persona senza completa identificazione».

[32] Cfr. PALMIERI, PARDOLESI, *Il codice in materia di protezione dei dati personali e l'intangibilità della «privacy» comunitaria*, cit.

[33] Cfr. R. ACCIAI, S. MELCHIONNA, *Le regole generali per il trattamento dei dati personali*, in ACCIAI (a cura di), *Il diritto alla protezione dei dati personali. La disciplina sulla privacy alla luce del nuovo Codice*, cit., 71; S. NIGER, *Il diritto alla protezione dei dati personali*, in MONDUCCI, SARTOR (a cura di), *Il codice in materia di protezione dei dati personali*, cit., 12-13 ss. In particolare sulle tecnologie volte a proteggere la privacy degli utenti, v. PASCUZZI, *Il diritto dell'era digitale*, cit., 77-82; B-J. KOOPS, R. LEENES, *'Code' and the slow erosion of privacy*, 12 *Mich. Telecomm. Tech. L. Rev.* 115 (2005).

Quanto sancito dall'art. 3 rappresenta una sorta di generale principio di indirizzo e di conformazione dell'azione tecnologica: esso afferma, infatti, che i sistemi informativi ed i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante dati anonimi o mediante opportune modalità che permettano di identificare l'interessato solo in caso di necessità. Da parte di alcuni è stato sostenuto che tale principio sembra imporre una prescrizione eccessiva e certamente volta a disciplinare in via preventiva l'utilizzazione di risorse informative da parte di soggetti pubblici e privati, con evidenti problemi di incostituzionalità in rapporto alla libertà individuale e d'impresa[34]. In realtà, esso, sebbene possa apparire di non facile comprensione nella sua genericità, trova la sua ragion d'essere nel fatto che alcuni rischi per la sicurezza di un sistema informativo possono essere evitati solo se a monte, al momento della programmazione della struttura informatica, ci si pone il problema di attuare le previsioni normative sulla protezione dei dati personali. La privacy può essere raggiunta solamente se il sistema è costruito in maniera tale da consentire la sua difesa[35].

L'importanza che riveste l'architettura informatica adottata per gestire il trattamento dei dati sanitari non è, dunque, di poco momento.

[34] Cfr. CORASANITI, *La sicurezza dei dati personali*, cit., 142.

[35] Un filone di ricerche interdisciplinari si dedica, appunto, allo studio dell'incorporazione di valori giuridici all'interno delle architetture digitali, seguendo un approccio interdisciplinare e giovandosi, così, dell'apporto di numerose e diverse scienze, l'economia, il diritto, la sociologia, l'informatica. Ci riferiamo al c.d. *value-sensitive design o value-centered design*. Per approfondimenti, v. V. MOSCON, *Rappresentazione informatica dei diritti tra contratto e diritto d'autore*, in *Ciberspazio e dir.*, 2010, 587 (in Rete: <http://eprints.biblio.unitn.it/archive/00001930>); S. BECHTOLD, *Value-centered Design of Digital Rights Management*, *Indicare*, 2004, in Rete: <http://www.indicare.org/tikiread_article.php?articleId=39>; B. FRIEDMAN, P.H. KHAN, A. BORINING, *Value Sensitive Design: Theory and Methods*, Technical Report, December 2002, in Rete <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.11.8020&rep=rep1&type=pdf>.

Condivisibile appare la scelta operata dal Garante Privacy, nel silenzio del legislatore, di non sposare alcuna (rigida) impostazione tecnologica ma di lasciare libero l'interprete di optare per il modello che meglio sia in grado di declinare all'interno dello scenario applicativo dato le regole indicate dal Codice e dall'Autorità Garante. Il principio di necessità trova così la sua collocazione ideale e la sua realizzazione in questo momento programmatico e creativo dei sistemi di FSE, proprio quando, appunto, si discute sul come costruire una piattaforma volta a gestire i dati sanitari dei pazienti-utenti-cittadini. La fase della programmazione è, ora, enfatizzata al massimo: c'è da augurarsi che quel precetto apparentemente sfuggente e senza un vero destinatario trovi allora quartiere nei tavoli che stanno gestendo la fase, complessa quanto necessaria, della digitalizzazione della servizio sanitario.

5. Fascicolo Sanitario Elettronico e biobanche di ricerca: una questione aperta

È opportuno dedicare ora spazio ad un approfondimento volto a tratteggiare possibili (ed auspicabili) interazioni tra i sistemi di FSE ed una realtà che si sta gradualmente affermando nel panorama nazionale ed internazionale, oltre a risultare di grande interesse per la scienza medica: le biobanche di ricerca[36]. La progressiva diffusione di queste

[36] Per approfondimenti sul tema delle biobanche di ricerca v. in generale J. KAYE, M. STRANGER (a cura di), *Principles and Practice in Biobank Governance*, Farnham UK - Burlington USA, 2009; M. MACILOTTI, *Biobanche* [aggiornamento-2011 in *Digesto civ.*, Torino, in corso di pubblicazione; ID., *Consenso informato e biobanche di ricerca*, in *Nuova giur. civ*, 2009, II, 153; ID., *Proprietà, Informazione ed interessi nella disciplina delle biobanche a fini di ricerca*, *id.*, 2008, 222; M. BARBARESCHI, S. COTRUPI, G.M. GUARRERA, *Biobanca: strumentazione, personale, analisi dei costi*, in *Pathologica*, 2008, fasc. 100, 139; M. MACILOTTI, U. IZZO, G. PASCUZZI, M. BARBARESCHI, *La disciplina giuridica delle biobanche*, in *Pathologica*, 2008, fasc. 100, 86; Y. BREGMAN-ESCHET, *Genetic Databases and Biobanks: Who Controls our*

ultime in ambito sanitario può portare a prefigurare favorevoli prospettive per la salute dell'uomo, determinando, al tempo stesso l'insorgenza di nuovi rischi e, di conseguenza, di interessi da tutelare.

Si distinguono diverse tipologie di biobanca, ognuna delle quali è finalizzata ad una specifica funzione, sia essa di ricerca, di indagine criminale, di supporto terapeutico, ecc. Tutte queste si caratterizzano per il fatto di prevedere per il loro funzionamento il trattamento di dati genetici, i quali, come i dati inerenti lo stato di salute, costituiscono a loro volta una sottocategoria dei c.d. dati sensibili, dai quali, però, si differenziano in ragione della loro peculiare natura: essi sono, infatti, inscindibilmente legati all'individuo dal quale provengono, per il fatto che ne raccontano le caratteristiche genetiche. Sono, dunque, idonei a rivelarne lo stato di salute presente, le predisposizioni a sviluppare o meno in futuro una determinata malattia, l'origine razziale ed etnica, il sesso e tutta una serie di informazioni (sensibili appunto) foriere di possibili discriminazioni nella vita sociale di ciascun individuo e gruppo. Le biobanche di ricerca interagiscono necessariamente con i dati genetici, essendo esse, fondamentalmente, «archivi» di tessuti e dati ad essi associati[37]. I campioni biologici conservati all'interno della biobanca sono, infatti, caratterizzati dalla compresenza di una doppia natura: quella prettamente materiale e quella informazionale, che, per l'appunto, è rappresentata dai dati genetici in essi contenuti e ad essi connessi. Posta, poi, la consumabilità del campione nella sua dimensione fisica, non è da escludere che, un domani, le biobanche diventino custodi dei soli dati raccolti, relativi, quindi, a campioni ormai scomparsi.

La relazione che qui si cerca di delineare rappresenta per certi aspetti una sorta di «salto nel buio», in quanto l'utilizzo simultaneo ed

Genetic Privacy?, 23 *Santa Clara Computer & High Tech. L.J.* 1 (2006).

[37] Per approfondimenti v. un recentissimo studio sul rapporto tra dati genetici e biodiritto C. CASONATO, C. PICIOCCHI, P. VERONESI (a cura di), *Forum BioDiritto - I dati genetici nel biodiritto*, Padova, in corso di pubblicazione.

in generale l'interazione tra le biobanche appena descritte ed il FSE rappresenta uno scenario del prossimo futuro di cui solo oggi si comincia a prefigurare il possibile avvento.

Questo sforzo predittivo permette ancora una volta di «accendere i riflettori» sul paziente, quale soggetto da cui derivano i campioni tissutali, raccolti e gestiti all'interno delle biobanche, ma anche come protagonista del flusso informazionale che deve al medesimo tornare come frutto dell'analisi posta in essere dalle biobanche di ricerca[38].

L'epoca che stiamo vivendo viene definita anche come «era post-genomica»: essa si caratterizza per il trattamento di enormi quantità di dati genetici degli individui[39]. Si assiste, per certi versi, al tentativo di determinare una stretta e sicura interrelazione tra le informazioni c.d. «genotipiche», che interessano quindi il genoma umano, e le informazioni c.d. «fenotipiche», le quali, invece, riguardano l'effettiva manifestazione di quei dati nella realtà sensibile.

Si va così affermando una nuova branca scientifica che viene definita «bioinformatica», la quale si connota per l'utilizzo delle tecnologie digitali nel campo della scienza biomedica al fine di fornire, in estrema sintesi, due tipi di strumenti: da un lato, quelli volti ad analizzare ed utilizzare i dati genetici per lo sviluppo di nuove terapie, medicine e metodologie di diagnosi mediche, e, dall'altro, quelli finalizzati a fornire informazioni che permettano di analizzare ed

[38] Le tecnologie digitali ed, in particolare, il c.d. web 2.0 non fanno che favorire, e per certi aspetti determinare, questo bisogno di sapere che contraddistingue l'utente della Rete e, più in generale, gli individui di quest'inizio terzo millennio.

[39] Cfr. in generale l'interessante documento COMITATO NAZIONALE PER LA BIOSICUREZZA E LE BIOTECNOLOGIE – GRUPPO DI LAVORO BIOINFORMATICA, *Linee guida per la definizione di una strategia per lo sviluppo del settore della bioinformatica in Italia con particolare attenzione all'ambito biomedico*, dicembre 2005, in Rete: <http://www.governo.it/biotecnologie/documenti/2.bioinformatica.pdf>; in dottrina v. S. RODOTÀ, *Tra diritto e società. Informazioni genetiche e tecniche di tutela*, in *Riv. crit. dir. priv*., 2000, 571.

utilizzare i dati genomici per il raggiungimento degli obiettivi sopra esposti[40].

Come si ricordava all'inizio di paragrafo, l'attenzione viene concentrata sul paziente. Si va affermando una tendenza volta a creare una nuova medicina personalizzata, in grado di riportare gli studi genetici direttamente al singolo individuo. Una diagnostica ed una terapia a ciò finalizzata si basa, fondamentalmente, su due aspetti: per un verso, l'individuazione dell'identità genetica e la conoscenza del c.d. «rischio genetico» (ovvero la possibilità del manifestarsi in futuro di una determinata malattia), e per l'altro la capacità predittiva che dall'analisi di questi deriva.

Questa nuova capacità che ci verrebbe consegnata dalle indagini genetiche permette di tracciare possibili interazioni con il FSE. Come è stato sottolineato in vari passi di quest'analisi, tali sistemi si caratterizzano per il trattamento di dati sanitari finalizzato ad assicurare un migliore processo curativo del paziente. Le stesse LG FSE sul punto così recitano:

> A garanzia dell'interessato, le finalità perseguite devono essere ricondotte quindi solo alla prevenzione, diagnosi, cura e riabilitazione dell'interessato medesimo[41].

Non sono, però, esplicitamente escluse dal Garante Privacy possibili altre modalità di utilizzo dei dati tramite un sistema di FSE per finalità di ricerca. Così le LG FSE sul punto:

> Eventuali, future utilizzazioni anche parziali del Fse o del *dossier* per ulteriori fini di ricerca scientifica, epidemiologica o statistica non sono

[40] Cfr. A. MONTI, *Bioinformatica e diritto d'autore. La conoscenza ha bisogno di codici aperti*, in *Ciberspazio e dir.*, 2006, 511; M. DEN BESTEN, *The Rise of Bionformatics*, Working Paper Series, aprile 2003, in Rete: <http://ssrn.com/abstract=1521649>.

[41] LG FSE, p. 2.9.

> di per se precluse, ma possono avvenire solo in conformità alla normativa di settore ed essere oggetto di preventiva e specifica attenzione, anche nei casi in cui – come accade per taluni progetti di Fse esaminati – la tenuta dell'elenco degli eventi sanitari riguardante un determinato interessato sia demandata a un'infrastruttura regionale[42].

Questo passaggio permette di sviluppare altre riflessioni sul tema della relazione tra FSE e biobanche di ricerca.

I sistemi di FSE consentono di avere la visione della storia clinica di un determinato soggetto; ciò, evidentemente, rafforza in maniera sensibile la capacità prognostica dell'operatore sanitario impegnato nell'apprestare il corretto processo curativo per il paziente che si è sottoposto alle sue cure. Ma vi è di più: la possibilità di analizzare in maniera aggregata il dettagliato quadro clinico di un paziente, aggiornato e completato dalle informazioni ricavabili dall'analisi genetica svolta sui suoi campioni tissutali, determinerebbe una crescita esponenziale della capacità predittiva con riferimento al suo decorso medico[43]. L'operatore sanitario potrebbe, così, porre in essere protocolli

[42] *Ibidem*, p. 2.11. In generale sul tema dell'utilizzo delle informazioni derivanti da sistemi EHR per finalità di ricerca medica v. D.J. WILLISON, *Use of Data from the Electonic Health Record for Health Research – current governance challenges and potentiale approaches*, marzo 2009, in Rete <http://www.priv.gc.ca/information/pub/ehr_200903_e.pdf>.

[43] In D.M. RODEN, J.M. PULLEY, M.A. BASFORD, G.R. BERNARD, E.W. CLAYTON, J.R. BALSER, D.R. MASYS, *Development of a Large-Scale De-Identified DNA Biobank to Enable Personalized Medicine*, in *Clinical Pharmacology and Therapeutics*, vol. 84, n. 3, 2008, 362, con specifico riferimento al rapporto tra biobanche ed EMR si legge: «coupling these biobanks to electronic medical record (EMR) systems has the potential to enable investigators in the field of genomics to search, record, and analyze phenotypic information pertaining to large numbers of patients in a "real word" context». Sull'auspicabile ritorno al donatore dei risultati della ricerca svolta presso le biobanche di ricerca v. L. SKENE, *Feeding Back Significant Findings to Participants and Relatives*, in KAYE, STRANGER (a cura di), *Principles and Practice in Biobank Governance*, cit., 161-175.

diagnostici veramente efficaci e mettere a punto innovativi *test* predittivi. La qual cosa avrà un effetto positivo con riferimento a due principali destinatari di queste rivoluzionarie tecniche diagnostiche: da una parte, in particolare, il singolo paziente che beneficerà di un'assistenza sanitaria adeguata al suo reale quadro clinico, presente e futuro; dall'altra, più in generale, il SSN il quale potrà approntare strategie di medio-lungo periodo realmente profilate su quelle che saranno le necessità della società del prossimo futuro (si immagini l'impatto che questo tipo di scenari potrebbe avere sui piani di investimento a livello nazionale e locale con riferimento ad una tra le spese più incisive nei bilanci degli enti statali).

Il quadro così delineato, però, non presenta solo aspetti positivi. Nel contesto anglosassone, con riferimento alla gestione dei dati genetici posto in essere dalle biobanche di ricerca, si utilizza spesso l'espressione *keeping it private*[44]: ciò sottolinea ancora una volta il fatto che la privacy dei soggetti che si sottopongono ai *test* genetici debba essere tutelata nel modo più robusto ed efficace possibile, vista la delicatezza dei risultati che tali esami sono in grado di produrre[45].

Diversi sono gli snodi cruciali su cui focalizzare l'attenzione[46].

---

[44] L'espressione è ripresa, con riferimento specifico alle tecniche di *de-identification*, da M. MALIAPEN, *Clinical Genomic Data Use: Protecting Patients Privacy Rights*, in *Studies in Ethics, Law, and Technology*, 2009, vol. 3, Issue 1, article 1, 3.

[45] In D. TOWNEND, M.J. TAYLOR, J. WRIGHTS, D. WICKINS-DRAZILOVA, *Privacy Interests in Biobanking: A Preliminary View on a European Perspective*, in KAYE, STRANGER (a cura di), *Principles and Practice in Biobank Governance*, cit., 137 : «the new genetic data processing possibilities are in potential conflict with these fundamental rights, because the real research value of biobanking and research using genetic data will be in its relation to the medical and environmental life-story of the data subject».

[46] In A. ZARABZADEH, R.W.G. BRADLEY, J. GRIMSON, *Ensuring Participatn Privacy in Networked Biobanks*, in KAYE, STRANGER (a cura di), *Principles and Practice in Biobank Governance*, cit., 177, vengono analizzati gli aspetti che occorre prendere in considerazione nel tutelare la riservatezza dei soggetti che si sottopongono ai *test* genetici; in particolare a p. 179 si legge: «ensuring the confidentiality of participant data at all times is an essential aspect of biobank operation».

Anzitutto appare fondamentale l'aspetto legato alla consapevolezza del soggetto interessato: questi deve essere adeguatamente informato degli scopi legati alla ricerca a cui si sta sottoponendo, delle modalità che caratterizzeranno i trattamenti posti in essere sui dati che lo riguardano e, nei limiti del possibile, delle probabili analisi future che potrebbero interessarli. Centrale, poi, allorquando si analizzi i profili della privacy degli individui, è il tema del consenso: non è questo né il luogo né il momento per approfondire un tema che impegna da anni i commentatori che si occupano di tale materia[47]. Preme qui soprattutto ricordare e sottolineare l'aspetto legato alla possibilità di revocare il consenso eventualmente prestato: in tal caso i campioni tissutali che contengono i dati genetici dovrebbero essere individuati e distrutti[48].

[47] Fiumi d'inchiostro sono stati versati su questa tematica, della quale la dottrina non ha mai smesso di interessarsi: v., fra i tanti, MACILOTTI, *Consenso informato e biobanche di ricerca*, cit.; R. JUSO, *Dati sensibili e consenso informato: profili costituzionali e legislativi*, in *Ragiusan*, 2004, fasc. 237, 6; M. CASINI, C. SARTEA, *La consulenza genetica in Italia: problemi, regole d consenso informato, trattamento dei dati genetici e privacy*, in *Medicina e morale*, 2009, 1121; C. CASONATO, *Il consenso informato. Profili di diritto comparato,* in C. CASONATO, T.E. FROSINI, T. GROPPI (a cura di), *Diritto pubblico comparato ed europeo*, 2009, 1052; R. BROWNSWORD, *Consent in Data Protection Law: Privacy, Fair Processing and Confidentiality,* in S. GUTWIRTH, Y. POULLET, P. DE HERT, C. DE TERWANGNE, S. NOUWT (a cura di), *Reinventing Data Protection?,* Dordrecht, 2009, 83; S. VICIANI, *Brevi osservazioni sul trattamento dei dati inerenti la salute e la vita sessuale in ambito sanitario*, in *Riv. critica dir. privato*, 2007, 315; B. GODARD, J. SCHMIDTKE, J.J. CASSIMAN, S. AYMÉ, *Data storage and DNA banking for biomedical research: informed consent, confidentiality, quality issues, ownership, return of benefits. A professional perspective,* in *European Journal of Human Genetic*s, 2003, vol. 11, suppl. 2, S88; S. VICIANI, *L'autodeterminazione «informata» del soggetto e gli interessi rilevanti (a proposito dell'informazione sul trattamento sanitario)*, in *Rass. dir. civ*., 1996, 272.

[48] L'effetto del ritiro del consenso è quello della distruzione immediata del campione e dei dati ad esso associati oppure della sua completa anonimizzazione, impedendone la riconducibilità al donatore, con tutte le perplessità sul punto già espresse *supra*. Questo è quanto stabilito anche dall'Autorizzazione al trattamento dei dati genetici del Garante Privacy del 22 febbraio 2007 la quale, al punto 6, afferma che «[…]In conformità all'art. 23 del Codice, il consenso resta valido solo se l'interessato è libero da ogni condizionamento o coercizione e resta revocabile liberamente in ogni momento. Nel

Infine, per ingenerare il corretto livello di fiducia su questi enti di ricerca, occorre garantire che la gestione degli accessi ai sistemi informativi, ed in particolare ai dati in essi trattati, sia regolata in maniera restrittiva e possibilmente limitata ai soli soggetti che sono entrati in contatto con i donatori al momento della raccolta dei campioni. Il passaggio subito successivo deve essere quello della c.d. «anonimizzazione», aspetto cruciale per la tutela della privacy dell'individuo che merita, invece, maggiori approfondimenti[49].

Tale procedimento consiste di fatto nella dissociazione, nella «raschiatura» (dall'inglese *scrubbing*), di alcuni dati identificativi dal campione tissutale al fine di assicurare la sua non identificabilità. Essa è posta in essere dalle stesse biobanche di ricerca o da parte di soggetti terzi fidati secondo modalità di *governance* che devono essere debitamente affrontate ed analizzate[50].

Si possono distinguere quattro approcci alla gestione della confidenzialità dei campioni tessutali conferiti alle biobanche[51]:

---

caso in cui l'interessato revochi il consenso al trattamento dei dati per scopi di ricerca, è distrutto anche il campione biologico sempre che sia stato prelevato per tali scopi, salvo che, in origine o a seguito di trattamento, il campione non possa più essere riferito ad una persona identificata o identificabile» (tale autorizzazione è stata da ultimo nuovamente prorogata sino al 30 giugno 2011 con deliberazione del Garante Privacy del 23 dicembre 2010). In generale v. G. HELGESSON, L. JOHNSSON, *The right to Withdraw Consent to Research on Biobank Samples,* in *Medicine, Health Care and Philosophy,* 2005, Vol. 8, No. 3, 315.

[49] Cfr. L. CAPLAN, *Consent and Anonymization in Research involving Biobanks,* in *Embo Reports,* 2006, Vol. 7, No. 7, 661.

[50] Con riferimento alla *governance* delle biobanche di ricerca, v. in prima battuta M. HÄYRY, R. CHADWICK, V. ÁRNASON, G. ÁRNASON (a cura di), *The Ethics and Governance of Human Genetic Databases, European Perspectives,* Cambridge, 2007; KAYE, STRANGER (a cura di), *Principles and Practice in Biobank Governance*, cit.

[51] Si v. ZARABZADEH, BRADLEY, GRIMSON, *Ensuring Participant Privacy in Networked Biobanks*, cit., 180, dove viene richiamato un documento della *National Bioethics Advisory Commission* del 1999 contenente le linee guida con riferimento alla confidenzialità delle informazioni gestite dalle biobanche: NATIONAL BIOETHICS ADVISORY COMMISSION, *Research Involving Human Biological Materials: Ethical Issues and Policy Guidance, vol. I: Report and Recommendation of the National Bio-*

- *Unidentified or anonymous samples*: le informazioni a carattere personale che potevano determinare l'identificabilità del soggetto non sono state richieste al momento della raccolta dei campioni tessutali, o, qualora ciò sia inizialmente accaduto, sono state subito cancellate: in tali casi non sussiste alcuna possibilità di rivelare informazioni confidenziali.
- *Unlinked or anonymized samples*: i campioni tissutali sono stati immagazzinati senza identificativi o codici individuali e vengono conferiti ai ricercatori del tutto privi di elementi che potrebbero far ricavare l'identità dei soggetti che si sono prestati al prelevamento del campione stesso. La biobanca o un soggetto terzo disinteressato al trattamento mantengono un *database* con le informazioni atte ad identificare i campioni.
- *Coded or linked or identifiable o*r *de-identified samples*: questa tipologia di campioni non è in grado di rivelare alcun tipo di informazione atta ad identificare i soggetti donanti; essi sono, però, accompagnati da un codice apposto dalla biobanca o da un suo rappresentante prima di essere resi disponibili ad attività di ricerca da parte di soggetti esterni. Il riabbinamento tra campione tessutale, anonimo, e dati identificativi è, pertanto, possibile.
- *Identified samples*: campioni tissutali che vengono forniti ai ricercatori provvisti dei dati identificativi dei donatori.

Il processo di *de-identification* è sicuramente quello maggiormente idoneo a garantire la privacy dei soggetti che partecipano alla ricerca. Tali procedure, quando a ciò sin dall'inizio predisposte, permettono, inoltre, la possibilità di riassociare il dato anonimizzato a quello identificativo[52]. L'aspetto non è di poco momento in questa

ethics Advisory Commission, Rockville, Maryland, 1999, 16-17. V. anche MALIAPEN, *Clinical Genomic Data Use: Protecting Patients Privacy Rights*, cit., 3.

[52] V. MALIAPEN, *Clinical Genomic Data Use: Protecting Patients Privacy Rights*, cit., 2, il quale appunto suddivide le tecniche di de-identificazione tra quelle che per-

riflessione volta a delineare un possibile rapporto tra biobanche e FSE. La c.d. *re-identification* consente, infatti, di riagganciare la patologia del singolo soggetto al suo *background* genetico, in tal modo permettendo che il flusso informazionale uscito dal paziente ritorni a questo attraverso il *medium* del suo FSE[53].

I rischi di una gestione non corretta di questo processo sono più che intuibili; i vantaggi, però, sono altrettanto evidenti e non fanno che valorizzare e provare quanto si sta qui sostenendo[54].

La relazione tra FSE e biobanche di ricerca appare ancora tutta da scoprire e da costruire. È presumibile attendersi che essa diverrà presto centrale nell'ambito della ricerca biomedica, in quanto, come più volte sottolineato, permette l'aggregazione di importantissime informazioni per il paziente: la ricerca genetica svolta sui suoi campioni e le patologie di cui soffre.

Il paziente è sempre più al centro del sistema salute: lo si è già constatato per quanto riguarda le piattaforme atte a gestire i suoi dati sanitari, lo si intuisce dagli scenari che sopra sono stati, seppure brevemente, delineati. La centralità del suo ruolo non deriva solo da motivazioni di carattere etico o giuridico; occorre anche tenere in considerazione il fatto che egli rappresenta la fonte stessa delle informazioni e, quindi, per primo necessita di acquisire la conoscenza

---

mettono la re-identificazione (*Patient De-identification System*) e quelle che la impediscono a priori (*Toolkit based Encryption System*).

[53] Un approfondimento a carattere generale sul tema della re-identificazione dei dati anonimi si rintraccia in M.V. DE AZEVEDO CUNHA, D. DONEDA, N. ANDRADE, *La re-identificazione dei dati anonimi e il trattamento dei dati personali per ulteriore finalità: sfide alla privacy*, in *Ciberspazio e dir*., 2011, 641.

[54] Cfr. MALIAPEN, *Clinical Genomic Data Use: Protecting Patients Privacy Rights*, cit., 4-5; TOWNEND, TAYLOR, WRIGHTS, WICKINS-DRAZILOVA, *Privacy Interests in Biobanking: A Preliminary View on a European Perspective*, cit., 137: «it allows the potential for understanding the origins of disease, and promises more tailored drug regimes, but at the same time in other hands it allows for risk assessments which could be used to express preferences between individuals or groups of individuals in employment or insurance».

del proprio stato di salute per meglio interagire con i servizi che il SSN gli fornisce. In questa prospettiva il FSE rappresenta una volta ancora lo strumento attraverso il quale le informazioni che riguardano il medesimo paziente tornano sotto il suo diretto controllo, garantendo così il concreto realizzarsi del principio di autodeterminazione.

Un altro interessante profilo è quello descritto dall'espressione c.d. «catene di fiducia» (*chain of trust and duty*). I sistemi di FSE già presentano il possibile rischio della c.d. disumanimazzione del rapporto medico-paziente: il contesto digitale farebbe perdere alla relazione tra questi due soggetti quella caratteristica che, invece, sin dagli albori della scienza medica, la contraddistingue. Anche nel tema che qui ci impegna occorre porre l'attenzione su qualcosa di simile. Il paziente entra in contatto con un determinato professionista, magari anche tramite un sistema di FSE, dietro il quale si inseriscono diversi altri soggetti (ad esempio laboratori, centri di ricerca e biobanche, cliniche) che svolgono attività di ricerca sui dati che lo riguardano. Il frutto di tali indagini torna al paziente per il tramite di una catena di soggetti che egli fondamentalmente non conosce ma di cui si fida in quanto ricoprono un determinato *status* all'interno di questa catena[55].

L'aspetto sicuramente più pregnante di significati della relazione tra FSE e biobanche è quello legato alla capacità predittiva che l'interazione tra questi due nuovi strumenti potrebbe assicurare. Mai come ora questa possibilità, questo riabbinamento tra la patologia specifica ed il *background* genetico del paziente permette di porre in essere protocolli predittivi e *test* diagnostici innovativi. Ci si interroga

[55] Per approfondimenti v. A.J. GREEN, *Chains of Trust and Duty in Health Information Management*, in *Studies in Ethics, Law, and Technology*, 2009, vol. 3, Issue 1, articolo 7, in part. 8 «in establishing systems where the public must be enabled to place trust in order to make potentially life changing decisions, but where their knowledge is insufficient to the task, i will be necessary to establish mechanism for trustworthiness and mechanisms for oversight and audit of those systems. It is reasonable to ask *Quis custodiet ipsos custodies?*».

spesso, e a ragione, sugli aspetti etici e morali che devono informare la raccolta di tessuti umani e sui regimi giuridici che la devono regolare. Non viene posta ancora abbastanza attenzione su quello che sarà l'impatto che la possibilità di prevedere, in termini sempre più oggettivi, il futuro, anche se solo con riferimento al proprio stato di salute, determinerà nei singoli individui e più in generale nella società stessa[56].

6. Digital divide *generazionale e sanità elettronica: il paradigmatico caso della delega alla gestione dei servizi offerti dal Fascicolo Sanitario Elettronico*

6.1 Premessa: i servizi on-line *e l'amministrazione digitale*

La fornitura di servizi *on-line* è un fenomeno in crescita esponenziale. Gli utenti di Internet sono ormai abituati ad impiegare portali che, sfruttando a pieno le potenzialità del web 2.0, permettono

[56] Gli antichi, con riferimento alla capacità di prevedere il futuro, parlavano di «divinazione»; con qualsiasi rituale o tecnica questa venisse posta in essere, la risposta che si otteneva non era mai direttamente e facilmente intellegibile e spesso nascondeva oscuri scenari. In chiusura del mio intervento al Convegno internazionale *Comparative Issues in the Governance of Research Biobanks*, tenutosi a Trento presso la Facoltà di Giurisprudenza il 7 e 8 maggio 2010 dal titolo *Biobanks as Electronic Gatekeepers of Personal Health Data: Open Issues* ebbi modo di richiamare sul punto un'attraente immagine letteraria (e cinematografica) tratta dal capolavoro di J.R.R. TOLKIEN, Il *Signore degli Anelli*: Galadriel, dama di Lórien, incontra lo *hobbit* Frodo, il portatore dell'anello, in una delle tappe del viaggio della «compagnia dell'anello»; l'elfo invita questi a guardare all'interno dello «Specchio di Galadriel», uno specchio magico che permette di vedere il futuro. Prima di concedergli tale possibilità però lo ammonisce con le seguenti, sibilline parole: «Molte cose domando allo Specchio di rivelare e ad alcuni posso mostrare ciò che desiderano vedere. Ma lo Specchio può anche spontaneamente mostrare delle immagini più strane e utili di quelle che desideriamo vedere; cose che furono, e cose che sono, e cose che ancora devono essere. Ma quali fra queste egli stia vedendo nemmeno il più saggio può sapere**.** Desideri ancora guardare*?*».

elevati livelli di interattività. È diventato normale – per molti è già un'irrinunciabile prassi quotidiana – gestire i propri conti correnti, i portafogli di investimento, la posta elettronica, le bollette del gas e della luce, le assicurazioni, il traffico con il proprio operatore telefonico e con il proprio fornitore di contenuti audio-video digitali, nonché le stesse relazioni sociali (si pensi ancora una volta alla straordinaria affermazione dei c.d. *social network*) attraverso piattaforme digitali ideate per consentirci di far leva sullo strumento informatico per governare situazioni, contatti ed interazioni che in precedenza potevano avere luogo esclusivamente in un contesto reale, caratterizzato dalla necessità di uno spostamento, e di un conseguente incontro fisico, e dal massiccio ricorso alla tecnologia della carta per documentare gli effetti giuridici di queste interazioni[57].

Anche le pubbliche amministrazioni hanno iniziato ad offrire ai propri cittadini-utenti servizi *on-line* volti a dare un nuovo volto al loro rapporto con questi nel mutato contesto tecnologico. Un rapporto che adesso si arricchisce di nuove forme di interazione, in un contesto ove i diritti che il cittadino vanta nei confronti della p.a. possono essere esercitati con minori costi di transazione e con modalità assai più incisive ed efficaci.

Si tratta di un processo che, a livello generale, è espressione di un fenomeno che da tempo ha preso ad essere designato alternativamente con un sintagma o con un'espressione anglofona ormai registrata nei dizionari della lingua italiana (rispettivamente: amministrazione digitale ed *e-government*). Da diversi lustri questo fenomeno è stabilmente inserito in cima all'agenda dei responsabili della funzione pubblica (ministeriale *in primis*, e – a cascata – territoriale nelle sue varie articolazioni), forte della promessa di realizzare una proporzione

[57] In generale sul passaggio dalla carta al *bit* vedi l'approfondimento ricco di spunti di riflessione di G. PASCUZZI, *Il diritto fra tomi e bit: generi letterari e ipertesti*, Padova, 1997.

inversa che appare irresistibile agli occhi dei pubblici decisori: tagliare i costi di esercizio del sistema, migliorando nel contempo l'efficacia dei servizi erogati agli utenti.

I servizi *on-line* vengono talvolta suddivisi in sotto-categorie: possono essere a carattere finanziario o non-finanziario; forniti ai cittadini o alle aziende; possono avere specifiche finalità (assistenza sanitaria, scopi educativi, servizi burocratici, ecc.). Una distinzione che appare però più utile ai nostri fini è quella che fa leva sulla differente relazione che si instaura con il cittadino: possiamo, pertanto, distinguere tra servizi a contenuto informativo (e per ciò stesso monodirezionali: il flusso informativo parte solo dal sito dal quale il servizio è erogato) e servizi che determinano una partecipazione dell'utente ai contenuti del sito web attraverso cui viene erogato il servizio *on-line*, e ancora servizi che determinano vere e proprie «transazioni», con le quali dati e informazioni sono oggetto di scambio e di interazione sistematica tra portale e utente[58]. Può osservarsi fin d'ora come sia proprio quest'ultimo tipo di servizi a presentare maggiori aspetti di criticità e complessità.

6.2 La delega quale atto necessario per la fruizione dei vantaggi connessi alla fornitura di servizi on-line*: il caso della sanità elettronica*

Nello scenario fin qui sommariamente abbozzato si vanno affermando nuove esigenze da parte degli utenti, i quali chiedono, e talvolta ormai pretendono, che il servizio a loro dedicato possa essere adattato con grande elasticità applicativa, per conformarsi al meglio alle caleidoscopiche necessità quotidiane di ciascuno. Poter «delegare» l'accesso alla pagina riservata all'interno del portale che ospita ed eroga il servizio rivolto all'utente di un'amministrazione digitale, nonché la

[58] Si v. CENSIS, *9° Rapporto: Le città digitali*, 2006, 5-6, in Rete: <www.censis.it>.

gestione di alcune delle operazioni interattive che all'interno dell'infrastruttura sono destinate a svolgersi, identifica una di queste nuove richieste a cui chi concepisce l'architettura informatica e le modalità di fornitura telematica dei servizi *on-line* è chiamato a dare riscontro[59].

Anche nel contesto digitale la possibilità di delegare l'accesso al servizio attraverso il quale compiere atti di gestione degli interessi del delegante risponde alle medesime ragioni che nel contesto reale hanno da sempre indotto il portatore di un interesse a conferire ad un altro soggetto, di propria fiducia, la gestione di quell'interesse, avente, o non, natura patrimoniale. Se ne può compiere un rapido inventario senza pretese di esaustività: il fattore tempo, ovvero l'urgenza di porre in essere attività che non si ha altrimenti modo di compiere (delegare ad un proprio familiare o ad una persona di propria fiducia il ritiro di quel referto che può avvenire solo in un momento coincidente con il proprio orario di lavoro); il fattore competenza, quando la consapevolezza di non essere esperti di un problema spinge a fidarsi di qualcuno più esperto di noi (delegare ad un addetto ai lavori la gestione di un patrimonio, attribuendo a quest'ultimo il potere di porre in essere atti di disposizione dello stesso)[60]; l'impossibilità (dovuta a *gap* fisici e sempre più spesso culturali) di utilizzare nuove tecnologie o inediti strumenti che in astratto sarebbero disponibili, ma che non si è

[59] Il presente approfondimento, parzialmente modificato, ha già trovato pubblicazione in U. IZZO, P. GUARDA, *Sanità elettronica, tutela dei dati personali e digital divide generazionale: ruolo e criticità giuridica della delega alla gestione dei servizi di sanità elettronica da parte*, in *Trento Law and Technology Research Group Research Papers*, n. 3, 2010, Trento, Università degli Studi di Trento, in Rete: <http://eprints.biblio.unitn.it/archive/00001921/>.

[60] La società Equitalia, ad esempio, consente a tutti gli intermediari abilitati ai servizi telematici dell'Agenzia delle Entrate di poter ricevere la delega per accedere all'estratto conto dei propri assistiti: v. <http://www.fiscoetasse.com/normativa-prassi/10860-estratto-conto-di-equitalia-cartelle-sotto-controllo-dei-professionisti-delegati.html>. Servizi simili sono disponibili anche su alcuni portali di *home banking*: la possibilità di delegare la gestione del proprio conto corrente *on-line* è però di regola concessa solo nei confronti di altri correntisti della stessa banca.

concretamente capaci di far funzionare (si pensi ai sempre più numerosi servizi *on-line* offerti dalle pubbliche amministrazioni, per i quali è divenuto ineludibile porsi il problema di fare in modo che la loro portata innovativa possa essere fruita dai cittadini più anziani che manifestano l'incapacità di utilizzare i nuovi strumenti).

Appare a questo punto necessario entrare nel vivo dell'argomento, valutando quali ostacoli si frappongono alla possibilità di concepire che i servizi di sanità elettronica ideati per migliorare la qualità delle prestazioni diagnostiche e terapeutiche rese a ciascun utente del SSN possano essere fruiti anche attraverso la cooperazione di un soggetto di propria fiducia, liberamente scelto e autorizzato dal beneficiario a gestire tale interazione, entro limiti ben definiti e sempre modificabili e con l'osservanza di tutta una serie di accorgimenti atti a tutelare il beneficiario stesso.

Il tema fatalmente incrocia gli sviluppi che la sanità elettronica sta conoscendo dal punto di vista della necessità di regolare le relazioni che i vari attori in essa coinvolti (distinguibili in linea generale in erogatori e destinatari delle prestazioni sanitarie) tendono sempre più ad instaurare sfruttando le potenzialità concesse dall'avvento del *bit*. In particolare, la discussione è sicuramente centrale anche con riferimento al tema dell'implementazione dei sistemi di FSE.

Un'ulteriore ragione che spinge ad una soluzione ragionata del problema che ci siamo posti è di matrice prettamente culturale. L'evoluzione tecnologica è scandita da ritmi rapidissimi: i cambiamenti sono talmente repentini che spesso solo le nuove generazioni (quelle che vengono definite dei «nativi digitali») riescono a tenerne il passo[61]. Il tradizionale modo di concepire il c.d. *digital divide*, che dividerebbe le regioni ricche del mondo, le quali hanno facile accesso alle

[61] L'espressione si deve a Mark Prensky, uno fra i massimi esperti sull'interazione tra tecniche di apprendimento e tecnologie digitali: v. PRENSKY, *Digital Natives, Digital Immigrants*, cit. Si v. anche U. GASSER, J. PALFREY, *Born Digital - Connecting with a Global Generation of Digital Natives*, Cambridge, MA, 2008.

tecnologie informatiche, da quelle povere, le quali invece ne sono spesso escluse, si colora di nuovi significati[62]: all'interno dello stesso contesto socio-culturale le vecchie generazioni appaiono sempre più in difficoltà nel governare le nuove forme di interazione che le tecnologie digitali permettono, in ciò subendo un vero e proprio distacco generazionale nei confronti dei più giovani, avvezzi, ed educati, al loro uso (ed abuso). Si può a tal proposito parlare di una sorta di «digital divide generazionale». Questo aspetto appare ancora più problematico nei contesti propri della sanità elettronica: per un verso, essa dovrebbe rappresentare un'efficace risposta all'aumento della richiesta di un servizio sanitario sempre migliore e più efficiente, dovuta, appunto, all'invecchiamento progressivo delle società occidentali; per l'altro, proprio i destinatari primi dei servizi che a tal proposito vengono forniti si vedono progressivamente esclusi dal poterli utilizzare a causa della loro «incapacità» tecnologica. Si parla al riguardo dell'esigenza di una sorta di alfabetizzazione informatica, unico investimento in grado di garantire la riuscita dei progetti di sanità elettronica. La possibilità di farsi assistere, in questa fase di transizione, da qualcuno di più esperto (e spesso di più giovane) appare essere una reale soluzione alle difficoltà generazionali create dalla rivoluzione tecnologica.

Dal punto di vista, infine, della protezione dei dati personali, all'interno di questi portali che forniscono servizi *on-line* l'utente riveste il ruolo di interessato al trattamento; coloro i quali forniscono il servizio ricoprono la funzione di «titolare del trattamento», coadiuvati da altri, eventuali, «responsabili del trattamento». La delega dell'accesso ad un servizio di FSE riguarda, evidentemente, anche il riconoscimento della possibilità in capo a terzi di gestire, e trattare i propri dati personali, concependoli quasi come «responsabili», in senso

[62] Si v. sul punto P. NORRIS, *Digital Divide: Civic Engagement, Information Poverty, and the Internet Worldwide*, Oxford, 2001, 3 ss.; v. anche M. KAGAMI, M. TSUJI, E. GIOVANNETTI (a cura di), *Information Technology Policy and the Digital Dived: Lessons for Developing Countries*, Cheltenham, 2004.

atecnico ovviamente, delle informazioni a carattere personale di cui possono venire a conoscenza. Anche questo aspetto andrà debitamente investigato, pur consci del fatto che la coperta delle regole positive risulta spesso troppo corta per coprire le situazioni sempre nuove che la realtà (tecnologica) ci consegna.

6.3 La delega dell'accesso al Fascicolo Sanitario Elettronico: altre considerazioni (con uno sguardo al passato)

Nella predisposizione di una piattaforma informatica idonea a gestire dati relativi ad eventi clinici occorsi ad un individuo e concepita per consentire a quest'ultimo, ad un tempo assistito del SSN ed interessato ai dati caratterizzanti tali eventi, di accedere al *repository* costituito nell'ambito di un FSE per inserirvi e registrarvi volta per volta nuovi dati, si presenta la necessità di disciplinare le modalità attraverso le quali l'utente interessato può delegare ad un altro soggetto di propria fiducia – non necessariamente a lui legato da vincoli familiari – l'accesso e la gestione dei dati relativi alla propria salute trattati nell'ambito di detto sistema.

Sul piano della sua validità quale atto negoziale, tale delega dovrebbe poter essere validamente rilasciata sia attraverso modalità tradizionali (delega tramite documento cartaceo per l'ottenimento di credenziali idonee, con validazione informatica effettuata presso gli uffici del soggetto titolare), sia impiegando modalità digitali, assistite da procedure considerate sicure (concessione del privilegio di accesso posta in essere utilizzando direttamente la piattaforma informatica).

Occorre premettere che nell'era cartacea l'assistito-interessato al trattamento dei dati sanitari che lo riguardano ha sempre goduto della facoltà di delegare a terzi il ritiro degli esami clinici, e, più in generale, di tutti i documenti cartacei contenenti dati sanitari che lo riguardano.

Un noto accorgimento a tutela della riservatezza del delegante,

invalso nel contesto predigitale, consiste nel consegnare al delegato la documentazione al cui ritiro costui è autorizzato dal delegante in una busta chiusa formalmente indirizzata a quest'ultimo (o al suo medico curante, per garantire che il dettato dell'art. 84 del Codice Privacy sia rispettato almeno formalmente). La trasposizione di questa facoltà nel contesto informatico presenta i consueti problemi connessi all'incorporazione di principi e regole giuridiche all'interno di un'architettura digitale[63].

Risultano immediatamente percepibili gli aspetti di sicuro vantaggio connessi alla possibilità di predisporre un sistema che garantisca ai soggetti che ne siano beneficiari la facoltà di delegare ad altri l'accesso al proprio FSE, onde tener conto della possibilità che l'interessato possa farsi assistere da un soggetto di propria fiducia per essere aiutato nel percorso terapeutico intrapreso, o, semplicemente, per essere meglio supportato nel processo di mantenimento del proprio stato di salute (si pensi al ruolo che a tal fine è spesso svolto nella vita di tutti i giorni da un figlio nei confronti del proprio genitore anziano, con i notevoli problemi che tale interazione pone quando il figlio e l'anziano genitore non risiedano nella medesima località).

Per altro verso, assumere atteggiamenti preclusivi in nome di posizioni di principio, tese ad escludere a priori la possibilità che nell'era digitale la gestione elettronica dei dati inerenti la salute dell'interessato possa essere oggetto di delega, apparirebbe un'irragionevole ingerenza nel potere di un individuo, in possesso della capacità di agire, di gestire sovranamente i propri interessi, con un evidente *vulnus* al suo diritto di autodeterminazione, tale da tradursi in una scelta di *policy* indirettamente volta a rallentare lo sviluppo della sanità elettronica.

[63] Cfr. PASCUZZI, *Il diritto dell'era digitale*, cit., *passim*; con particolare riferimento alla privacy v. GUARDA, ZANNONE, *Towards the Development of Privacy-Aware Systems*, cit.

Ciò detto, è agevole immaginare i timori che, nel passaggio dalla logica cartacea a quella digitale, possono prendere corpo, riflettendo il sostanziale aumento del rischio che, nel nuovo contesto, verrebbe a gravare sul delegante digitale.

Nel contesto cartaceo, infatti, la delega attiene al ritiro di un documento determinato contenente dati sanitari; diversamente, l'atto che abilita un soggetto a fare le veci dell'interessato delegante all'interno di un sistema di archiviazione e gestione in remoto dei dati inerenti la propria salute assumerebbe carattere generale, aumentando esponenzialmente i rischi connessi a possibili trattamenti illeciti dei dati sanitari in esso contenuti.

Occorre nondimeno riflettere attentamente sull'esistenza di una serie di accorgimenti e di regole tecnologiche che permettono di gestire questo rischio, riportandolo entro dimensioni di accettabilità ed evitando di optare per soluzioni regolative che – in un atteggiamento di rifiuto dell'innovazione – finirebbero per rendere eccessivamente complesso e poco fruibile nel quotidiano il meccanismo di delega.

Come sempre accade nel caso di scelte regolative che attengono a scenari ove la volontà giuridicamente rilevante di un soggetto e i suoi effetti concreti sono mediati dal *bit*, una soluzione estrema che accarezzi l'idea di dire semplicemente no alla possibilità che l'interessato deleghi ad un altro soggetto la gestione del proprio interesse ai dati inerenti la propria salute innescherebbe il rischio assai concreto che le sue credenziali di accesso al sistema di sanità elettronica finiscano per essere comunque irritualmente rese note alla persona di cui l'interessato abbia fiducia, con l'effetto perverso (e gravissimo in una prospettiva di *policy* regolativa) di annullare la coincidenza fra credenziali (e dunque l'identità informatica dell'interessato) e colui al quale queste realmente corrispondono[64].

[64] I sistemi di autenticazione rappresentano il punto nodale di una piattaforma che, per fornire i propri servizi, tratta informazioni dotate di un elevato livello di sensibilità.

6.4 Riflessioni sulla qualificazione giuridica della delega all'accesso

Al prezzo di apparire didascalici, ma al fine di risultare maggiormente comprensibili anche a chi non è un esperto della materia, occorre delineare, almeno nei suoi tratti essenziali, la cornice giuridica entro cui inserire la possibilità che un terzo deleghi a terzi l'accesso al FSE contenente dati che lo riguardano, descrivendo sia pur sommariamente gli aspetti fondamentali degli istituti giuridici coinvolti.

La possibilità da parte di un soggetto (in grado di intendere e di volere[65]) di delegare ad un altro il compimento di una o più attività che questi ha il potere di porre in essere in nome e per conto dell'interessato

---

Gli strumenti che gestiscono l'attività di identificazione di un soggetto all'interno della piattaforma informatica si basano sull'utilizzo di credenziali personali, che fanno sì che il sistema riconosca il soggetto che le immette quale utente, consentendo da quel momento a quest'ultimo, tramite i permessi associati a quelle credenziali, di porre in essere un determinato *set* predefinito di trattamenti. Affrontare consapevolmente il problema della delega dell'accesso al FSE significa, anche e soprattutto, contrastare sin dalle prime fasi di progettazione dell'intero sistema il «malcostume», purtroppo diffuso, che si sostanzia nella cessione delle proprie credenziali a terzi al fine di permettere loro la gestione della «pagina» a sé dedicata. Dietro la sua parvenza di pratico *escamotage*, questa prassi in realtà presenta aspetti di spiccata pericolosità e criticità in quanto dissocia, o comunque confonde, l'identità virtuale del soggetto, che il sistema registra quale autore di determinate attività, e l'identità reale del soggetto che materialmente le pone in essere. È il caso di ricordare che, oltre alle prescrizioni contenute nell'Allegato B del Codice Privacy pp. 1-11 sui sistemi di autenticazione informatica, qualora configurabile, l'art. 615-*quater* del Codice Penale sanziona la detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici: «Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a lire 10 milioni».

[65] Diversa, e per certi aspetti più semplice, è la questione relativa ai soggetti che non godono della capacità di agire e per i quali l'ordinamento prevede già forme di «delega» nel compimento di atti anche di forte impatto nella vita del soggetto (v. le forme di rappresentanza legale).

si esprime attraverso l'istituto della rappresentanza[66], se è vero che

> si ha rappresentanza ogniqualvolta taluno agisce per conto e nell'interesse di un altro[67].

È ben noto che la rappresentanza è ammessa nell'ambito del diritto patrimoniale ed è esclusa per i c.d. atti personalissimi (quali ad es. il riconoscimento di un figlio, il testamento)[68]. Quando è consentito l'intervento di un terzo per il compimento di un atto tipico del diritto familiare (si pensi, ad esempio, al matrimonio per procura), quest'ultimo riveste il ruolo di semplice portavoce, che non collabora alla formazione della volontà del primo: è il caso del c.d. *nuncius*[69].

Il potere rappresentativo ai sensi dell'art. 1388 c.c. fa leva su quattro presupposti[70]: innanzitutto il conferimento in capo al rappresentante di un qualche potere rappresentativo; in secondo luogo il rappresentante deve necessariamente agire rispettando i limiti dei poteri a lui devoluti; allo scopo di attivare il meccanismo della rappresen-

---

[66] In generale sulla rappresentanza, V. ROPPO, *Il contratto*, in G. IUDICA, P. ZATTI (a cura di), *Trattato di diritto privato*, Milano 2001, 257-326, e i riferimenti ivi contenuti; W. D'AVANZO, voce *Rappresentanza*, in *Nov. Dig. it*., Torino, 1967, 801 ss.; U. NATOLI, *Rappresentanza (dir. civ.)*, in *Enc. dir*., XXVIII, Milano, 1987; A. TRABUCCHI, *La rappresentanza*, in *Riv. dir. civ*., 1978, I, 584.

[67] In ROPPO, *Il contratto*, cit., 257.

[68] Così M. GRAZIADEI, *Mandato*, in *Digesto civ*., Torino, 1994, vol. XI, 154, 160: «Il riferimento all'oggetto del contratto opera anche in sede di determinazione delle cause di nullità del mandato. Non può essere conferito incarico per il compimento di atti personalissimi, ed è nullo il mandato con cui si attribuisce al mandatario la facoltà di designare la persona del donatario, o di determinare l'oggetto della donazione (art. 778, co. 1)».

[69] Per approfondimenti, ROPPO, *Il contratto*, cit., 262-263; U. COSSU, *Nuncius*, in *Digesto civ*., Torino, 1995, vol. XII, 3; G. CIAN, *L'intervento di un nuncius nella formazione delle fattispecie negoziali*, in *Studium iuris*, 1996, 13; G. GIUSTI, *La figura giuridica del "nunzio"*, in *Nuovo dir*., 1986, 417.

[70] T. ONIDA, F. ROMANI, S. SANTORO, *Agenti elettronici e rappresentanza volontaria nell'ordinamento giuridico italiano*, in *Informatica e dir*., 2003, 197, 202-203.

tanza, inoltre, il rappresentante deve sempre agire nell'interesse del rappresentato; infine, occorre che l'atto negoziale sia posto in essere dal rappresentante in nome del rappresentato (la c.d. spendita del nome).

Il potere di rappresentanza può trovare la sua fonte nella legge (si parla allora di rappresentanza legale: si pensi ad esempio a quella degli incapaci o delle persone giuridiche)[71]; oppure nell'esplicita volontà di un soggetto che si realizza mediante un negozio giuridico (c.d. rappresentanza volontaria)[72]: la procura[73]. Questa è definibile come un atto unilaterale rivolto a terzi costitutivo di poteri: essa si accompagna in genere al mandato o a un contratto similare, ma può esserne priva. La procura di per sé stessa ha efficacia nei confronti dei terzi al fine di attestare l'esistenza ed il contenuto dei poteri delegati.

Essa può essere, poi, «speciale», quando riguarda il compimento di uno o più atti determinati (e tutti gli atti indispensabili per il loro compimento), o «generale», quando si estende al compimento di tutti gli atti relativi alla generalità degli affari del rappresentato, ovvero a un gruppo di suoi affari.

La procura va tenuta distinta dalla figura del mandato, il quale, ai sensi dell'art. 1703 c.c., è

> il contratto col quale una parte si obbliga a compiere uno o più atti

[71] In tema, *ex plurimis*, V. DI GREGORIO, *Rappresentanza legale*, in *Dig. civ*., Torino, XVI, 293; P. PATRIZIA, *In tema di rappresentanza legale dei minori*, in *Giur it*., 1989, 1055.

[72] In tema, fra i molti, A. SALOMONI, *La rappresentanza volontaria*, in P. CENDON (a cura di), *Contratti*, IX, Torino, 2000, 57; V. DE LORENZI, *La rappresentanza diretta volontaria. Problemi e soluzioni alla luce dell'analisi economica del diritto*, in *Contr. impr*., 1997, 595; L. MOSCO, *La rappresentanza volontaria nel diritto privato*, Napoli, 1960.

[73] Per approfondimenti ROPPO, *Il contratto*, *cit*., 271-274; R. VARANO, *Forma della procura e contratto concluso dal rappresentante*, in *Notariato*, 1998, 116; V. DE LORENZI, *Procura*, in *Digesto civ*., Utet, 1997, vol. XV, 317; A. POZZI, *Procura*, in *Enc. giur*., XXIV, Roma, 1991; L. BIGLIAZZI GERI, *Procura (dir. priv.)*, in *Enc. dir*., XXXVI, Milano, 1987.

giuridici per conto dell'altra.

Nel caso di mandato con procura, gli effetti giuridici degli atti compiuti dal mandatario in nome del mandante si verificano direttamente in capo al mandante. Il mandato può anche essere senza rappresentanza o con rappresentanza impropria o indiretta. Con riferimento al contenuto, possiamo avere poi il c.d. «mandato speciale» quando viene determinato il tipo di atti da compiere e delle operazioni gestorie; si ha, invece, il c.d. «mandato generale» allorquando non si specifica il tipo di atti da realizzare ed il contratto è potenzialmente idoneo a ricomprendere ogni tipo di affare o una serie indeterminata di affari. Al mandato speciale si applica quanto previsto dall'art. 1708 c.c.:

> Il mandato comprende non solo gli atti per i quali è stato conferito, ma anche quelli che sono necessari al loro compimento.

Il mandato generale, invece, non comprende gli atti eccedenti l'ordinaria amministrazione, salvo che essi siano espressamente indicati (v. art. 1708, co. 2, c.c.)[74].

La differenza tra i due negozi giuridici è evidente. Il mandato è un contratto ed in quanto tale consiste in un atto bilaterale: da esso deriva innanzitutto l'obbligo per il mandatario di compiere uno o più atti giuridici per gestire l'affare che egli si è assunto (nel nostro caso, quindi, la gestione dei trattamenti operabili accedendo con le proprie credenziali ai profili di autorizzazione connessi alla persona dell'interessato delegante nell'ambito di un FSE). La procura, invece,

[74] Per approfondimenti sull'istituto del mandato, v. G. CASSANO, M. GIANDOMENICO (a cura di), *I contratti di intermediazione - Mandato, agenzia, mediazione, contratto estimatorio, commissione, procacciamento d'affari, concessione di vendita, franchising, intermediazione finanziaria*, Padova, 2009; M. GRAZIADEI, *Mandato*, in *Riv. dir. civ*., 1997, II, 147; ID., *Mandato in diritto comparato*, in *Digesto civ*., Torino, 1994, vol. XI, 192; U. CARNEVALI, *Mandato (diritto civile),* in *Encicl. giur. Treccani*, Roma, 1990, vol. XIX.

rappresenta un atto unilaterale e attribuisce un potere verso i terzi. Della questione relativa alla forma di tali atti si dirà più avanti.

Quando i poteri del rappresentante saranno cessati, egli avrà l'obbligo di restituire il relativo documento a chi gli ha attribuito la procura.

Riportando la trattazione al nostro caso, possiamo, dunque, configurare l'atto attraverso il quale un soggetto esprime la propria volontà affinché un terzo possa accedere al suo FSE come un mandato con annessa procura speciale. Al mandatario viene, infatti, delegato il potere rappresentativo di compiere tutti gli atti propri di un particolare gruppo di affari del mandante: la gestione del suo FSE.

6.5 Problemi di forma: dal contesto cartaceo a quello digitale

> Il diritto si serve delle tecnologie disponibili al fine di perseguire determinati obiettivi (ad esempio la certezza delle relazioni giuridiche). I medesimi obiettivi possono essere raggiunti utilizzando tecnologie differenti. Al cambio di tecnologia corrisponde un cambio delle regole (perché, ad esempio, occorre disciplinare i presupposti di operatività delle diverse tecnologie)[75].

L'attività di documentazione e di archiviazione delle informazioni è stata sin qui svolta attraverso il supporto cartaceo. La validità degli atti compiuti e la certezza del loro contenuto sono stati gestite attribuendo valore e significato giuridico a documenti che rappresentavano graficamente la volontà dei soggetti coinvolti. Da un certo punto di vista, si può dire che la sicurezza di tale forma di comunicazione ed archiviazione di informazioni si basava sul carattere indelebile che si imprimeva sulla carta e sulla firma autografa, la quale valeva a sancire l'appropriazione dei contenuti del documento da parte del soggetto che la vergava. Il mutare delle tecnologie rende necessario individuare

[75] In PASCUZZI, *Il diritto dell'era digitale*, cit., 95.

nuove regole che permettano a forme informatizzate di gestione dei documenti di ottenere i medesimi risultati assicurati dalla tecnologia della carta[76].

Circoscriviamo il nostro ambito di indagine al problema che qui ci impegna ed analizziamo le regole che gestiscono il conferimento del potere di rappresentanza nel contesto reale, per verificare la possibilità di replicare la disciplina così enucleata, profilandola al contesto digitale.

Al fine di rendere sicura la procura ed evitare possibili falsificazioni delle informazioni contenute, l'art. 1392 c.c. sancisce che

> La procura non ha effetto se non è conferita con le forme prescritte per il contratto che il rappresentante deve concludere.

Pertanto se il contratto richiede una particolare forma per la validità, la sua conclusione non ha effetto per il rappresentato se la procura non è redatta secondo la stessa forma dell'atto principale. La

[76] Non è questa la sede per affrontare l'analisi dell'evoluzione normativa inerente la documentaristica informatizzata. Basti qui ricordare che il legislatore italiano aveva, tra i primi in Europa, colto la sfida, riconoscendo validità giuridica agli «atti, dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici e telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici» (v. art. 15, co. 2, l. 15 marzo 1997, n. 59). Altro momento decisivo in questo percorso era stato rappresentato dai numerosi interventi normativi dettati anche e soprattutto dalla necessità di recepire la Direttiva 1999/93/CE relativa al quadro comunitario per le firme elettroniche. La normativa ora vigente nel nostro ordinamento per quanto concerne la disciplina del documento informatico e delle firme elettroniche è contenuta nel CAD e dalle norme del d.P.R. 28 dicembre 2000, n. 445 non abrogate dal suddetto codice. Per approfondimenti sull'evoluzione del concetto di documento informatico v. PASCUZZI, *Il diritto dell'era digitale*, cit., 95-139; A. GRAZIOSI, *La nuova efficacia probatoria del documento informatico*, in *Riv. trim. dir. proc. civ.*, 2003, 53; S. PATTI, *L'efficacia probatoria del documento informatico*, in *Riv. dir. proc.*, 2000, 60; F. FERRARI, *La nuova disciplina del documento informatico*, in *Riv. dir. proc.*, 1999, 129; A. GENTILI, *Documento informatico e tutela dell'affidamento*, in *Riv. dir. civ.*, 1998, fasc. 3, 2, 163.

forma in tale contesto migliora la qualità delle informazioni che nella procura sono contenute e ne riduce la possibile falsità, ingenerando il corretto affidamento nel soggetto che la riceve. La procura scritta, in particolare, garantisce anche la provenienza e la veridicità formale del contenuto. Ma la funzione della forma non è solo quella di autenticazione e certificazione del suo contenuto; essa diviene anche strumento per facilitare l'assolvimento dell'onere della prova, che grava sul terzo[77].

Ora interroghiamoci su cosa avviene nella pratica allorquando decidiamo di delegare a terzi il compimento di una determinata attività. Nello specifico, come già sopra evidenziato, poniamo il caso della delega a terzi del ritiro di un referto clinico presso un ospedale o un laboratorio d'analisi. La volontà di conferire ad altri il potere di farsi rappresentare nello svolgimento dell'attività richiesta trova sua espressione nella procura scritta che generalmente compiliamo, accompagnandola, per aumentarne la certezza, con una fotocopia del documento di identità. La principale «misura di sicurezza» di tale forma di delega è rappresentata dalla sottoscrizione del rappresentato che valida in tale maniera il documento e ne garantisce la bontà.

Prima di affrontare l'analisi della trasposizione di questo tipo di attività, che si svolge interamente utilizzando le regole proprie della tradizione cartacea, al contesto digitale aggiungiamo qualche altro particolare utile a decidere quale possa essere la soluzione più appropriata.

La delega dell'accesso ad un servizio *on-line*, nel peculiare caso del FSE, implica il riconoscere a terzi il potere di trattare i propri dati personali. La disciplina in materia di protezione dei dati personali all'art. 8, co. 1, Codice Privacy sancisce che:

[77] Sulla forma della procura, v. in prima battuta DE LORENZI, *Procura*, cit., 327; ROPPO, *Il contratto*, cit., 272; P. CAPARRELLI, *Forma volontaria e forma della procura*, in *Giur. it*., 1975, I, 1, 1155.

> I diritti di cui all'articolo 7 [Diritti dell'interessato al trattamento] sono esercitati con richiesta rivolta senza formalità al titolare o al responsabile, anche per il tramite di un incaricato, alla quale è fornito idoneo riscontro senza ritardo.

Il Codice Privacy richiede anche una determinata formalità per l'esercizio di tale delega. Innanzitutto all'art. 9, co. 2, prescrive che

> Nell'esercizio dei diritti di cui all'articolo 7 l'interessato può conferire, per iscritto, delega o procura a persone fisiche, enti, associazioni od organismi. L'interessato può, altresì, farsi assistere da una persona di fiducia.

Inoltre, con riferimento all'eventuale identificazione, al comma 4 dello stesso articolo si prevede che:

> L'identità dell'interessato è verificata sulla base di idonei elementi di valutazione, anche mediante atti o documenti disponibili o esibizione o allegazione di copia di un documento di riconoscimento. La persona che agisce per conto dell'interessato esibisce o allega copia della procura, ovvero della delega sottoscritta in presenza di un incaricato o sottoscritta e presentata unitamente a copia fotostatica non autenticata di un documento di riconoscimento dell'interessato. Se l'interessato è una persona giuridica, un ente o un'associazione, la richiesta è avanzata dalla persona fisica legittimata in base ai rispettivi statuti od ordinamenti[78].

[78] Il Codice Privacy prevede, quindi, modalità analoghe a quelle già in vigore nell'ambito dei rapporti con la pubblica amministrazione; l'art. 38, co. 3, d.P.R 28 dicembre 2000, n. 445 «Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (Testo A)», infatti prevede che: «Le istanze e le dichiarazioni sostitutive di atto di notorietà da produrre agli organi della amministrazione pubblica o ai gestori o esercenti di pubblici servizi sono sottoscritte dall'interessato in presenza del dipendente addetto ovvero sottoscritte e presentate unitamente a copia fotostatica non autenticata di un documento di identità del sottoscrittore. La copia fotostatica del documento è inserita nel fascicolo. Le istanze e la copia fotostatica del

Certamente la delega di cui tratta il Codice Privacy riguarda un caso alquanto limitato e ristretto (il solo esercizio dei diritti che l'interessato al trattamento può far valere nei confronti del titolare del trattamento) rispetto a quello qui indagato della delega alla gestione della posizione di interessato nell'ambito di un FSE. È altrettanto vero, però, che quanto sopra descritto conferma la necessità di alcuni requisiti formali per l'atto di delega di cui in queste pagine si cerca di ricostruire le caratteristiche.

Torniamo, ora, al problema evidenziato all'inizio di questo paragrafo. Si è detto che nel contesto cartaceo la procura a svolgere una determinata attività, quale nel nostro caso il ritiro di un referto presso una struttura ospedaliera, richiede la formalità del documento sottoscritto dal delegante, accompagnata dalla fotocopia di un documento di riconoscimento. Come si traduce tutto questo nel contesto digitale? Quali sono le regole che disciplinano il valore legale dei documenti redatti in modalità informatiche?

L'art. 20, co. 1, del CAD sancisce che

> il documento informatico da chiunque formato, la memorizzazione su supporto informatico e la trasmissione con strumenti telematici conformi alle regole tecniche di cui all'art. 71 sono validi e rilevanti agli effetti di legge, ai sensi delle disposizioni del presente codice[79].

---

documento di identità possono essere inviate per via telematica; nei procedimenti di aggiudicazione di contratti pubblici, detta facoltà è consentita nei limiti stabiliti dal regolamento di cui all'articolo 15, comma 2 della legge 15 marzo 1997, n. 59». Per approfondimenti, v. G. SALZANO, *I diritti dell'interessato*, in J. MONDUCCI, G. SARTOR (a cura di), *Il codice in materia di protezione dei dati personali. Commentario sistematico al d.lgs. 30 giugno 2003, n. 196*, Padova, 2004, 19-33; L. LA BATTAGLIA, *Commento art. 9*, in BIANCA, BUSNELLI (a cura di), *La protezione dei dati personali. Commentario al d.lgs. 30 giugno 2003, n. 196 ("Codice Privacy")*, cit., 215-224; S. PARDINI, *ibidem*, 224-230.

[79] Il comma 1-*bis* dell'art. 20 CAD specifica, inoltre, che: «L'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, tenuto conto delle sue caratteristiche oggettive di

Il comma terzo dello stesso articolo prevede che debbano essere emanate specifiche regole tecniche, ai sensi dell'art. 71 CAD, atte a gestire la formazione, la trasmissione, la conservazione, la copia, la duplicazione, la riproduzione e la validazione temporale, nonché relative alla generazione, apposizione e verifica di qualsiasi tipo di firma elettronica avanzata.

Ai nostri fini, interessa sottolineare come il documento informatico sottoscritto con firma elettronica avanzata, qualificata o digitale soddisfi il requisito legale della forma scritta e si presuma riconducibile al titolare del dispositivo di firma (art. 21, co. 2, CAD)[80]. Il CAD dedica il Capo V (Dati delle pubbliche amministrazioni e servizi in rete), sezione III, proprio ai servizi in rete offerti dalle p.a. e indica delle regole utilissime alla soluzione del problema che ci impegna. Cominciando dalla modalità di accesso ai servizi erogati in rete, l'art. 64 CAD prevede, per i casi in cui sia richiesta l'identificazione informatica, l'utilizzo della carta d'identità elettronica (CIE) o della carta nazionale dei servizi (CNS). Il comma secondo dello stesso articolo, alleggerendo subito la previsione, sancisce che le pubbliche amministrazioni possono consentire l'accesso ai servizi in rete da esse erogati che richiedono l'identificazione informatica anche con strumenti diversi dalla CIE e dalla CNS, purché questi permettano di accertare l'identità del soggetto il quale richiede l'accesso (v. ad esempio i vari sistemi di *strong authentication*)[81].

---

qualità, sicurezza, integrità ed immodificabilità, fermo restando quanto disposto dall'articolo 21».

[80] Il documento, invece, a cui è apposta una firma elettronica è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità (art. 21, co. 1, CAD).

[81] Con la novella del CAD ad opera del già citato d.lgs 235/2010 è stato definitivamente abrogato il termine, previsto al comma terzo dell'art. 64 CAD, che sanciva il momento oltre il quale non sarebbe più stato consentito l'accesso ai servizi *on-line* delle p.a. (31 dicembre 2007) con strumenti diversi dalla CIE e dalla CNS. Questo era stato ogni anno oggetto di proroga, l'ultima delle quali aveva previsto come termine per il

Appurata la modalità di accesso al servizio *on-line* che vede una preferenza per l'utilizzo della CIE e della CNS ma permette l'utilizzo di altri sistemi di autenticazione ritenuti idonei alla luce del trattamento oggetto del servizio, occorre ora chiedersi se ed in che modo siano presentabili istanze e dichiarazioni per via telematica, quali la delega dell'accesso al proprio FSE, alle pubbliche amministrazioni. L'art. 65 CAD detta la disciplina sul punto:

> Le istanze e le dichiarazioni presentate alle pubbliche amministrazioni per via telematica ai sensi dell'articolo 38, commi 1 e 3, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, sono valide:
> a. se sottoscritte mediante la firma digitale, il cui certificato è rilasciato da un certificatore accreditato;
> b. ovvero, quando l'autore è identificato dal sistema informatico con l'uso della carta d'identità elettronica o della carta nazionale dei servizi, nei limiti di quanto stabilito da ciascuna amministrazione ai sensi della normativa vigente;
> c. ovvero quando l'autore è identificato dal sistema informatico con i diversi strumenti di cui all'articolo 64, comma 2, nei limiti di quanto stabilito da ciascuna amministrazione ai sensi della normativa vigente, nonché quando le istanze e le dichiarazioni sono inviate con le modalità di cui all'articolo 38, comma 3, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445[82];

---

passaggio ai nuovi strumenti di identificazione il 31 dicembre 2010: v. art. 1, co. 5, d.l. 30 dicembre 2009, n. 194 convertito con modificazioni in legge 26 febbraio 2010, n. 25.

[82] L'art. 38, comma 3, del d.P.R. 28 dicembre 2000, n. 445 così recita: «3. Le istanze e le dichiarazioni sostitutive di atto di notorietà da produrre agli organi della amministrazione pubblica o ai gestori o esercenti di pubblici servizi sono sottoscritte dall'interessato in presenza del dipendente addetto ovvero sottoscritte e presentate unitamente a copia fotostatica non autenticata di un documento di identità del sottoscrittore. La copia fotostatica del documento è inserita nel fascicolo. Le istanze e la copia fotostatica del documento di identità possono essere inviate per via telematica; nei procedimenti di aggiudicazione di contratti pubblici, detta facoltà è consentita nei limiti stabiliti dal regolamento di cui all'articolo 15, comma 2 della legge 15 marzo 1997, n. 59. (L)»

> c-*bis*) ovvero se trasmesse dall'autore mediante la propria casella di posta elettronica certificata purché le relative credenziali di accesso siano state rilasciate previa identificazione del titolare, anche per via telematica secondo modalità definite con regole tecniche adottate ai sensi dell'articolo 71, e ciò sia attestato dal gestore del sistema nel messaggio o in un suo allegato. In tal caso, la trasmissione costituisce dichiarazione vincolante ai sensi dell'articolo 6, comma 1, secondo periodo. Sono fatte salve le disposizioni normative che prevedono l'uso di specifici sistemi di trasmissione telematica nel settore tributario[83].

Le istanze e le dichiarazioni così inviate o compilate sono da considerarsi equivalenti a quelle sottoscritte con firma autografa apposta in presenza del dipendente addetto al procedimento (v. art. 65, co. 2, CAD). Possono essere individuati i casi in cui è richiesta la sottoscrizione mediante firma digitale con decreto del Ministro per la pubblica amministrazione e l'innovazione e del Ministro per la semplificazione normativa, su proposta dei Ministri competenti per materia (v. art. 65, co. 1-*bis*, CAD).

Tiriamo le fila di quanto sopra esposto e riportiamo l'analisi al caso della delega dell'accesso ad un sistema di FSE. Per presentare validamente una dichiarazione volta a rappresentare la procura dei poteri che si trasferiscono al rappresentante in modalità informatica all'interno di una piattaforma informatica occorrerà che questa sia sottoscritta utilizzando la firma digitale ai sensi dell'art. 65, co. 1, lett. a, CAD (dal lato cittadino tale opzione risulta, per ora, difficilmente utilizzabile se rapportata alla totalità dei possibili utenti), oppure – soluzione di più facile applicazione – sia posta in essere per mezzo di un sistema informatico che utilizza come metodi di identificazione la CIE o la CNS (art. 65, co. 1, lett. b, CAD), ovvero tramite l'utilizzo di

[83] La seconda parte della lett. c e la lett. c-*bis* del co. 1 sono state inserite nel CAD dal d.lgs. 235/2010.

strumenti di identificazione diversi ma ugualmente idonei ad accertare l'identità del soggetto che richiede l'accesso (v. art. 65, co. 1, lett. c, CAD, il quale richiama gli strumenti di cui all'art. 64, co. 2, CAD)[84].

6.6 Ruolo del titolare del trattamento e sicurezza del sistema

Come già ricordato, gli innovativi strumenti di sanità elettronica, ed in particolare il web 2.0, forniscono nuove modalità di interazione tra la piattaforma-servizio e gli utenti-pazienti; emerge sempre più l'esigenza di consentire a quest'ultimi non solo le stesse possibilità e facoltà che il contesto reale già riconosceva loro, ma anche tutte quelle che dovessero derivare da un efficace realizzazione nel contesto digitale della loro personalità.

In tale scenario il titolare del trattamento, ovvero, in definitiva, colui il quale gestisce le piattaforme informatiche che forniscono questi nuovi servizi e ne verifica l'affidabilità e la sicurezza, recita un ruolo di primo piano. Egli dovrà, infatti, essere in grado di garantire che tutte le forme di interazione di cui si caratterizza il rapporto tra utente-paziente e portale avvengano secondo modalità e canali idonei a prevenire qualsiasi tipo di problema legato, in senso lato, alla sicurezza dei dati. A tal fine, appare necessario adottare una soluzione tesa a contemperare gli interessi coinvolti ed in grado di contemplare la possibilità di delegare la gestione dei propri dati sanitari in base ai principi di seguito enucleati.

Anzitutto, occorre dare completa espressione al principio di autodeterminazione del paziente-utente e costruire un sistema in grado di garantire la modularità della possibilità di delega, permettendo di limitare quest'ultima sia con riferimento a particolari tipi di dati (ad

[84] Infine, altra possibilità per la presentazione di istanze e dichiarazioni alla p.a. è quella che si basa sull'utilizzo della posta elettronica certificata, secondo quanto previsto dall'art. 65, co. 1, lett. c-*bis*, CAD.

esempio permettendo l'accesso ai soli referti, o ai soli dati relativi alle automisurazione, ecc.), sia con riguardo al tipo di operazioni effettuabili (ad esempio, consentendo solo l'accesso a video, la stampa, la sola immissione di dati, ecc.). Il concetto di modularità si ritrova come costante nei principi ispiratori di un sistema di FSE: prevedere la possibilità di gestire le operazioni che la piattaforma concede all'utente-paziente in maniera tale da conformarle alle reali esigenze dello stesso rappresenta sicuramente uno strumento per bilanciare correttamente gli interessi in gioco.

Altro principio cardine del sistema è quello della temporaneità. Il titolare del trattamento, nel fornire il servizio *on-line* e, di conseguenza, nel trattare i dati, è obbligato ad implementare, oltre alle misure minime previste dall'art. 34 Codice Privacy e dall'Allegato B dello stesso (ad esempio un sistema di autenticazione sicuro, un sistema di gestione delle credenziali, ecc.), pure le misure idonee e preventive atte a ridurre il rischio di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, avendo avuto riguardo alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento (v. art. 31 Codice Privacy). Orbene: nel configurare la propria piattaforma in modo tale da consentire la delega dell'accesso a terzi della pagina personale, il titolare deve porsi il problema di assicurare il massimo livello di affidabilità del sistema ponendo grande attenzione al fatto che i rischi che incombono sui dati sanitari così gestiti siano ridotti al minimo. Una soluzione potrebbe essere quella di prevedere che la delega debba essere temporanea in modo da garantire periodicamente la verifica dell'attualità della volontà delegante, sottoponendo a conferma il consenso inizialmente espresso (ad esempio: ogni tre mesi, riprendendo in via analogica quanto previsto dall'Allegato B del Codice Privacy con riferimento all'obbligo di modifica della *password* di accesso al sistema

nel caso di dati sensibili). Non possiamo, però, ignorare il fatto che anche questa soluzione, la quale da un punto di vista teorico appare facilmente applicabile, presenti poi nella realtà diverse criticità: se, come nella maggior parte dei casi, ci si può aspettare che i fruitori più interessati a questo tipo di servizio saranno soggetti anziani (i quali saranno interessati a non rimanere esclusi dall'utilizzo di uno strumento così utile e potente quale il FSE), occorre porsi il problema che questi incontreranno, nel rinnovare la delega digitalmente, le stesse difficoltà che li hanno inizialmente spinti a delegare ad altri l'accesso al proprio fascicolo[85]. La durata del termine temporale di validità della delega, qualora si ritenesse opportuno prevederla, potrà essere estesa a periodi più lunghi in relazione alle scelte che si prenderanno anche con riferimento agli altri dispositivi che verranno adottati per rendere sicuro questo nuovo tipo di trattamento. Un punto dovrà, comunque, sempre rimaner saldo: la delega può essere revocata in ogni momento. Il sistema dovrà prevedere la possibilità di bloccare l'intervento del terzo all'interno della propria «pagina» secondo modalità semplificate e di facile fruizione (ad esempio, attraverso il portale, o un servizio telefonico con chiamata ad un numero verde sempre attivo in grado di garantire un elevato livello di sicurezza nell'identificazione del soggetto chiamante[86]).

Infine, è fondamentale che il sistema garantisca la piena tracciabilità (evidentemente non modificabile dall'utente) delle operazioni di trattamento compiute dal delegato sui dati di pertinenza del delegante (registrazione, accesso in visualizzazione e stampa). Si può immaginare a tal fine che ogni dato dell'interessato delegante registrato nel FSE dell'interessato delegante possieda una sorta di *record* delle operazioni

[85] Certamente rimarrebbe sempre la via del rinnovo della delega in modalità cartacea: il delegato potrebbe premurarsi di far firmare la nuova procura al delegante e di portarla, con allegata una fotocopia del documento di identità, presso un ufficio dell'Azienda sanitaria a ciò preposto.

[86] V. ad esempio i sistemi di blocco telefonico delle carte di credito.

di trattamento che su di esso sono state svolte (magari automaticamente generato dal sistema stesso) con l'indicazione dell'identità del trattante e dell'ora dell'operazione di trattamento.

Il titolare del trattamento (la ASL, nel caso di FSE) dovrebbe, dunque, predisporre un sistema informatico idoneo a consentire l'implementazione fluida di questi tre principi garantendone il rispetto e l'osservanza nella realtà quotidiana.

Un'ultima riflessione con riferimento alla qualifica formale che il soggetto delegato finirebbe per assumere all'interno di un sistema così congegnato. Il paziente-utente-delegante riveste all'interno dei nomenclatori previsti dalla normativa sulla privacy la qualifica di interessato al trattamento che il sistema concepito dal titolare-ASL pone in essere con riferimento ai suoi dati. A quest'ultimo spetta la possibilità di delegare – vuoi mediante un atto di preposizione (responsabile del trattamento), vuoi attraverso un'autorizzazione (incaricato al trattamento) ad un soggetto interno alla propria organizzazione, o esterno alla stessa (responsabile esterno, con i suoi eventuali incaricati) – alcuni dei compiti e delle responsabilità che la legge, appunto, gli riserva. All'interessato è riservato un ruolo del tutto passivo all'interno del sistema.

La possibilità di delegare l'accesso al proprio FSE da parte dell'assistito apre, però, a nuove ed inaspettate forme di responsabilità con riferimento ai dati gestiti dal sistema, determinando il sorgere di nuovi rapporti obbligatori con riguardo alla gestione degli stessi dati sanitari. Premesso che i dati archiviati nel sistema sarebbero posti nella titolarità della ASL, in quanto soggetto responsabile del sistema informatico messo a disposizione (attraverso interfaccia accedibile in remoto) dell'assistito, il quale, a sua volta, in questo quadro non potrebbe che assumere le vesti di interessato, si sarebbe tentati, allora, di inquadrare il delegato utilizzando l'inesistente categoria dell'«incaricato dell'interessato», in quanto questi sarebbe legittimato a trattare i

dati personali e sensibili del delegante – evidentemente all'interno di una piattaforma a tal fine configurata dal titolare – proprio in forza di una sorta di autorizzazione, delimitata (modularità) e circoscritta anche temporalmente (temporaneità).

6.7 Considerazioni di sintesi

La delega alla gestione dei servizi *on-line* di sanità elettronica rappresenta un banco di prova sul quale testare al massimo livello i rischi che le nuove forme di interazione permesse dal contesto digitale presentano. I problemi che nello specifico la delega dell'accesso al proprio FSE fa emergere possono apparire in prima battuta quasi insuperabili: la possibilità di concedere a terzi la gestione addirittura dei propri dati sanitari sembra indurre qualsiasi fornitore di servizi ad «invertire la marcia» ed a non imboccare la strada che potrebbe portare a scelte rischiose e dalle prospettive future incerte.

Nel corso di questa breve trattazione si sono delineate le regole che potrebbero guidare la predisposizione di un servizio orientato in tal senso. Descriviamo di seguito alcune ragioni che dovrebbero indurre a trovare una soluzione positiva al quesito che ci siamo inizialmente posti.

Anzitutto, va tenuto presente che il riconoscere al paziente la possibilità di delegare la gestione del servizio *on-line* a lui dedicato rappresenta una misura di sicurezza per l'intero sistema. L'utente dei servizi di sanità elettronica, specialmente se anziano o, comunque non del tutto avvezzo all'uso dei nuovi sistemi informatici (si veda quanto sostenevamo sopra con riferimento alle difficoltà dei c.d. «immigrati digitali» in un *digital divide* che appare sempre più su base generazionale), è di fatto incentivato, proprio per usufruire di una possibilità così profilata sulle sue esigenze mediche, a concedere ad altri le proprie credenziali di accesso. Queste, però, identificheranno

all'interno del sistema il delegato come l'utente-paziente stesso (delegante) facendo perdere l'associazione tra atto compiuto nel contesto digitale e reale identità di chi l'ha posto in essere. Con la ragionevole certezza che ciò avverrà, assurdo sarebbe non affrontare il problema; potremmo anzi sostenere che il non essersi posti l'eventualità di questo accadimento possa essere valutata come una mancata predisposizione di una misura di sicurezza idonea e preventiva ad evitare un danno per i dati gestiti dal sistema sicuramente prefigurabile.

Inoltre, e ricollegandoci a quanto appena esposto, aspetto centrale per tutti i servizi che l'era digitale offre è quello della necessità di provvedere ad un'alfabetizzazione informatica a favore dei sempre più numerosi utenti della Rete. Giorno dopo giorno il computer non rappresenta più solamente uno strumento attraverso il quale porre in essere semplici operazioni che agevolano il nostro vivere quotidiano. Le tecnologie digitali hanno dimostrato una tale capacità invasiva da condizionare fino nei più reconditi dettagli l'esistenza umana: l'affermazione dei diritti propri della convivenza civile sempre più viene mediata, molto spesso garantita, dallo strumento informatico il quale deve incorporare principi e valori del nostro contesto sociale. Per traghettare un numero crescente di persone verso l'utilizzo degli strumenti informatici, i quali per molti aspetti potenziano la possibilità di essere cittadini attivi e di fruire al meglio dei propri diritti, occorre fornire agli utenti, specialmente se più anziani o meno «educati» all'uso di *personal* computer, delle applicazioni all'interno dei vari servizi atte ad agevolarli in questa fase di transizione: la delega dell'accesso nei confronti di un soggetto più preparato e del quale ci si fida può sicuramente rappresentare uno di questi strumenti al fine di colmare un *gap* culturale, e spesso generazionale, che rischia di creare nuove aree di analfabetismo (informatico).

Tale ultima considerazione, infine, è pure cruciale per la definitiva affermazione dei servizi di sanità elettronica oggetto di

finanziamenti sempre più cospicui da parte del governo nazionale e dell'Unione europea, i quali sperano in tal modo di potenziare il servizio sanitario riuscendo, nel contempo, a contenerne la spesa. «Fiducia» è la parola chiave dei servizi *on-line*. Essa si costruisce solamente se il sistema riesce a far sentire a proprio agio l'utente, permettendogli di acquisire gradatamente le abilità.

CONCLUSIONI

Lo studio dei sistemi di FSE contenuto nelle precedenti pagine non può che essere parziale ed esemplificativo. Si tratta di un tema che dovrà essere ulteriormente esplorato ed approfondito. Tuttavia il ragionamento fin qui svolto offre già alcune chiavi di lettura utili a sciogliere i nodi problematici di maggiore rilievo.

Ci si accinge ad utilizzare un nuovo strumento tecnologico continuando a ragionare ed organizzarsi secondo gli schemi suggeriti dai documenti medici cartacei. Il cambiamento tecnologico, invece, obbliga in primo luogo ad un mutamento concettuale ed organizzativo.

Molti sono gli aspetti problematici ed i rischi da tenere in considerazione nell'affrontare in maniera critica e consapevole lo studio delle applicazioni offerte dalle tecnologie digitali.

La stessa definizione di FSE rappresenta un punto cruciale da cui non si può prescindere. Il Garante Privacy ha preferito, con un approccio che appare condivisibile, non imporre una determinata scelta architetturale. L'Autorità ha, invece, fornito un quadro giuridico-concettuale all'interno del quale inserire diversi progetti accomunati dall'idea di base della condivisione logica di dati prodotti e trattati da parte di più autonomi titolari del trattamento. Il modo in cui tale quadro giuridico-concettuale troverà applicazione e gli scenari nei quali verrà declinato rappresentano una delle future sfide della sanità elettronica. All'interno di tale cornice, assume un'importanza fondamentale il ruolo che si deciderà di attribuire all'utente-paziente delle architetture informatiche di FSE. Il ripensamento dei servizi sanitari passa per il riconoscimento al cittadino di una posizione centrale all'interno del sistema, cioè di un ruolo da protagonista nelle scelte che lo riguardano. La for-

tuna di questo nuovo strumento si misurerà nella sua capacità di tradurre nel contesto digitale le garanzie che il mondo non digitale, grazie anche all'eredità dell'esperienza e della tradizione, riconosce all'utente. La partita decisiva si giocherà sul piano dell'interattività che le tecnologie informatiche offrono nei più disparati ambiti dell'agire umano e di cui tanto si avverte l'esigenza all'interno di un rapporto – quello tra medico e paziente – che, da sempre, si basa su una relazione di fiducia.

I sistemi di FSE rappresentano uno strumento estremamente potente per tracciare aspetti delicatissimi (quali sono quelli sanitari) della storia di una persona: non si ha più a che fare con un singolo documento posto sotto il controllo di pochi operatori sanitari, ma con un fascicolo che contiene informazioni che circolano, vengono modificate, aggiornate, arricchite da numerosi soggetti, tra i quali, ora, anche il paziente. Uno strumento non condannato all'oblio, cartaceo, del passato, ma tendenzialmente sempre attivo, disponibile, *on-line*. Alle enormi potenzialità che il FSE presenta con riferimento alla cura dei singoli fanno, però, da contraltare gli evidenti rischi di abuso cui esso può essere oggetto.

All'interno del fenomeno che è stato qui esaminato, si delineano in modo evidente due interessi confliggenti che possono rappresentare a loro volta due direttrici evolutive delle piattaforme atte al trattamento dei dati sanitari. Questo contrasto, in realtà, si ritrova anche ad un livello più generale, in quanto caratterizza molti dei fenomeni tipici della società dell'informazione.

Da un lato, si trova l'interesse del singolo individuo ad un controllo sempre più attento e capillare dei dati personali che lo riguardano e che circolano nelle reti di comunicazione. L'avvento delle tecnologie digitali, come è stato più volte ribadito, ha determinato una crescita dell'importanza attribuita al cittadino-utente nell'ambito di una società sempre più condizionata dalla rivoluzione informatica. I sistemi di FSE rappresentano un perfetto esempio di questa tendenza che porta a con-

cepire l'intera infrastruttura attorno non ai titolari-gestori di essa, bensì agli interessi espressi dal singolo soggetto che all'interno del sistema stesso opera. Su questa linea argomentativa, il principio di autodeterminazione non rappresenta altro che l'estrinsecazione giuridica di una capacità che l'utente nel mondo digitale acquisisce autonomamente. Tutto ciò in un sistema di FSE si traduce nella necessità che la scelta su quali informazioni inserire, i livelli di condivisione e le varie tecniche di oscuramento dei dati siano gestiti direttamente dal paziente attraverso lo strumento del consenso, che, in maniera sempre più modulare e complessa, realizza le volontà dell'utente all'interno dell'infrastruttura informatica. Emerge, così, chiaramente l'interesse del singolo ad avere finalmente voce in capitolo sul processo curativo che lo riguarda e ad acquisire un ruolo di gestore diretto della banca dati che contiene le sue informazioni sanitarie, con poteri di accesso e modifica veramente innovativi rispetto a quelli tradizionali.

Dall'altro lato, si pone, però, un interesse contrastante con quello appena tratteggiato. Esso si sostanzia nella necessità di attribuire poteri di controllo e di accesso, con riferimento alle nuove piattaforme digitalizzate, distribuendoli tra le varie strutture sanitarie che hanno come dovere-obbligo la cura del paziente-interessato e, più in generale, la tutela della salute di tutti. Abbiamo avuto modo di sostenere quanto il reale punto di forza di questi strumenti sia rappresentato dalla possibilità di aggregare una mole di informazioni prima impensabile, rendendola disponibile, nella maniera più rapida ed agevole possibile, agli operatori sanitari che di esse necessitino per finalità di prevenzione e cura. A tale esigenza si lega poi quella di carattere superindividuale che si estrinseca nell'interesse all'implementazione di un servizio sanitario sia a livello nazionale che regionale il più efficace ed efficiente possibile: la disponibilità di flussi informativi completi ed aggiornati garantisce alle ASL, ed in generale al SSN, la possibilità di elaborare valide strategie di prevenzione e cura di tutti gli assistiti e di programmare i piani

di investimento relativi a servizi sanitari sempre più profilati sulle reali esigenze degli utenti. Evidenza di ciò sono i vari progetti che a livello internazionale stanno emergendo e che dimostrano un interesse reale da parte delle autorità competenti nel governare i processi evolutivi dei servizi sanitari del terzo millennio.

La soluzione del contrasto tra la tutela del diritto alla privacy dell'utente e l'interesse superindividuale alla salute di tutti appare, allora, l'obiettivo teorico-pratico da raggiungere per coloro che si occupano di sanità elettronica e si trovano chiamati, nei vari ambiti di competenza, a garantire che l'evoluzione di nuovi strumenti digitalizzati si compia sempre nell'alveo dei principi e delle regole che caratterizzano i nostri ordinamenti giuridici. È necessario, cioè, trovare un ragionevole punto di saldatura tra gli interessi sopra descritti, avendo a mente che essi non si pongono come alternativi e che la realizzazione dell'uno non determina necessariamente l'annullamento dell'altro. Anzi, una loro corretta convergenza è, in realtà, in grado di assicurare tutti i vantaggi che i servizi offerti dalla digitalizzazione promettono nel concreto rispetto dei diritti dei singoli. Il ruolo del paziente-utente va, pertanto, sicuramente rafforzato anche tramite il riconoscimento di poteri sempre più incisivi all'interno delle piattaforme che trattano i suoi dati. Ciò, soprattutto, con riferimento alla necessità che egli divenga attore consapevole, sia da un punto di vista tecnico-informatico che, latamente, medico-scientifico (torna il concetto già citato di «alfabetizzazione informatico-sanitaria»). Occorre, però, superare un'interpretazione eccessivamente forzata del principio di autodeterminazione, che si estrinsechi in una sorta di signoria assoluta sul dato, a favore di una soluzione che veda prevalere l'interesse, generale e superiore, del SSN nel suo complesso.

La forza centripeta dei sistemi di FSE spinge a rivedere la questione della protezione dei dati personali secondo una nuova prospettiva. In questo contesto si materializza uno scenario complesso: la circo-

lazione delle informazioni è il frutto di decisioni e scelte rimesse non solo alla volontà del singolo, ma anche e soprattutto a varie strutture e soggetti, magari organizzati in differenti livelli gerarchici e dislocati in diversi punti geografici. Questo fa emergere l'esigenza di dare contenuto ad un'altra soluzione innovativa a cui si è fatto spesso cenno nel corso della trattazione: la nozione di co-titolarità.

Guardando al tema da una prospettiva più ampia, il tradizionale rapporto medico-paziente fornisce già alcune indicazioni valide alla soluzione dei problemi ora ricordati. Spesso si parla di comunità anche per riferirsi all'insieme degli utilizzatori di Internet. Il concetto di comunità rimanda a quello di un'organizzazione sociale implicante un ordine composto da soggetti che, all'interno del sistema, ricoprono ruoli ed assumono responsabilità diverse in ragione dell'esperienza e delle competenze che essi possiedono. L'ambito medico riproduce questo tipo di struttura organizzativa. Infatti, per quanto il paziente debba essere sempre più favorito nell'accesso, consapevole, ai processi curativi che lo riguardano, le decisioni in merito ad essi devono pur sempre essere condizionate dall'imprescindibile parere del medico, il quale, all'interno di un sapere e di relazioni codificate, diviene mentore qualificato del percorso che il paziente vorrà seguire per migliorare la propria condizione psico-fisica. Il rapporto medico-paziente si basa su una necessaria asimmetria informativa che risponde ad un differente livello di competenza scientifica.

Certamente i rischi che il nuovo trattamento dei dati sanitari tramite sistemi di FSE presenta non sono completamente azzerabili. Il diritto, però, è in grado di governare gli aspetti problematici appena descritti. Il sicuro vantaggio in termini di cura dei singoli e di tutela della salute pubblica impone di accettare la sfida. La soluzione al problema passa per un approccio interdisciplinare capace di far dialogare tra loro medici, giuristi, tecnologi, economisti, sociologi, in generale tutti i soggetti coinvolti nella costruzione di una piattaforma che, alla luce di un

progetto chiaro e grazie al confronto tra saperi diversi, sia in grado di incorporare ed esprimere principi e regole, valorizzando il ruolo del paziente, ma riuscendo, al contempo, ad assicurare la tutela della salute di tutti.

La bontà della scelta operata sarà dimostrata dai risultati in termini di efficacia del servizio sanitario, fidelizzazione degli utenti-pazienti nei confronti dello stesso nonché di analisi costi e benefici delle piattaforme.

Per concludere, merita di essere citato un passo del famoso giuramento di Ippocrate – nella sua versione classica – il quale mostra come il tema della riservatezza dei dati sanitari del paziente, trattati nell'ambito dell'attività medica, fosse anche allora sentito sebbene in un contesto sociale e tecnologico molto diverso:

> E quanto vedrò e udirò esercitando la mia professione, e anche al di fuori di essa nei miei rapporti con gli uomini, se mai non debba essere divulgato attorno, lo tacerò ritenendolo alla stregua di un sacro segreto[1].

[1] Nella sua versione originale: «Ἃ δ' ἂν ἐν θεραπείῃ ἢ ἴδω, ἢ ἀκούσω, ἢ καὶ ἄνευ θεραπηίης κατὰ βίον ἀνθρώπων, ἃ μὴ χρή ποτε ἐκλαλέεσθαι ἔξω, σιγήσομαι, ἄῤῥητα ἡγεύμενος εἶναι τὰ τοιαῦτα»: testo greco e traduzione italiana tratti da IPPOCRATE, *Antica Medicina. Giuramento del medico*, a cura di M. VEGETTI, Milano, 1998, 130-131. Riecheggia tra queste righe – scritte pare nel IV secolo a.c. – quello che noi moderni chiameremmo principio di necessità. Il giuramento moderno è stato deliberato dal Comitato Centrale della Federazione Nazionale Ordini Medici Chirurghi e Odontoiatri il 23 marzo 2007 e sul punto così prevede: «di osservare il segreto professionale e di tutelare la riservatezza su tutto ciò che mi è confidato, che vedo o che ho veduto, inteso o intuito nell'esercizio della mia professione o in ragione del mio stato».

BIBLIOGRAFIA

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

ACCIAI R. (a cura di), *Il diritto alla protezione dei dati personali. La disciplina sulla privacy alla luce del nuovo Codice*, Santarcangelo di Romagna, 2004

ACCIAI R., *La tutela della privacy ed il s.s.n.*, in *Ragiusan*, 2003, fasc. 225/226, 20

ACCIAI R., MELCHIONNA S., *Le regole generali per il trattamento dei dati personali*, in R. ACCIAI (a cura di), *Il diritto alla protezione dei dati personali. La disciplina sulla privacy alla luce del nuovo Codice*, Santarcangelo di Romagna, 2004, 71

ALPERT S., *Smart Card, Smarter Policy. Medical Records, Privacy, and Health Care Reform*, 23 *The Hastings Center Report* 13 (1993)

ANDERSON R., *Security Engineering. A Guide to Building Dependable Distributed Systems*, Wiley, 2001, in Rete: <http://www.cl.cam.ac.uk/%7Erja14/book.html>

ANDREOLI G., BELTRAMI D., CARAMAZZA M., CASCIOLI S., MARINI M.G., RAIMONDI M. (a cura di), *L'impatto dell'informatizzazione sulle aziende sanitarie lombarde e le relative implicazioni su formazione e addestramento degli operatori*, in Rete: <http://www.istud.it/up_media/ricerche/equal_san.pdf>

ANTON J.J., YAO D.A., *Standard-Setting Consortia, Antitrust, and High-Technology Industries*, 64 *Antitrust L.J.* 247 (1995)

ARTHUR W.B., *Positive Feedbacks in the Economy*, 262 *Scientific American* 92 (1990)

ASKLAND A., *A Wonderland of Disposable Facts*, in *Studies in Ethics, Law, and Technology*, 2009, vol. 3, Issue 1, art. 6

ASSCHER L., *'Code' as Law. Using Fuller to Assess Code Rules*, in E. DOMMERING, L. ASSCHER (a cura di), *Coding Regulation. Essays on the Normative Role of Information Technology*, The Hague, 2006, 61

AZZONI G.M., *Regola tecnica*, in *Dig. civ.*, Torino, 1997, vol. XVI, 470

BAICE P., *La cartella clinica tra diritto di riservatezza e diritto di accesso*, in *Resp. civ*., 2008, 169

BAKARDJIEVA M., SMITH R., *The Internet in Everyday Life: Computer Networking from the Standpoint of the Domestic User*, 3 *New Media & Society* 67 (2001)

BAKARDJIEVA M., *Virtual Togetherness: An Everyday-life Perspective*, 25 *Media, Culture & Society* 291 (2001)

BARBARESCHI M., COTRUPI S., GUARRERA G.M., *Biobanca: strumentazione, personale, analisi dei costi*, in *Pathologica*, 2008, fasc. 100, 139

BARILÀ E., CAPUTO C., *Problemi applicativi della legge sulla privacy: il caso delle cartelle cliniche*, in *Politica del diritto*, 1998, 275

BARNI M., *Diritti-doveri, responsabilità del medico. dalla bioetica al biodiritto*, Milano, 1999

BARON R.J., FABENS E.L., SCHIFFMAN M., WOLF E., *Electronic Health Records: Just around the Corner? Or over the Cliff?*, in *Ann. Intern. Med*., 2005, 143

BASSI A., *La cartella clinica come atto amministrativo*, in *Dir. ed economia assicuraz.*, 1992, 753

BECHTOLD S., *Value-centered Design of Digital Rights Management*, *Indicare*, 2004, in Rete: <http://www.indicare.org/tikiread_article.php?articleId=39>

BENEDETTI A.M., *L'autonomia privata di fronte "diritto privato delle regioni"*. Corte cost. sent., 13 novembre 2009, n. 295, in *Contratti*, 2010, 113

BENOLIEL D., *Technological Standards, INC. Rethinking Cyberspace Regulatory Epistemology*, 92 *Cal. L. Rev*. 1069 (2004)

BERGHELLA F., *Guida pratica alle nuove misure di sicurezza per la privacy*, Roma, 2003

BERNARD A., *La protection de l'intimité par le droit privé. Éloge du ragot ou comment vices exposés engendrent vertu*, in CURRAP (a cura di), *Le for intérieur*, Parigi, 1995, 155, in Rete <http://www.u-picardie.fr/labo/curapp/revues/root/35/alain_bernard.pdf_4a081e8ad4544/alain_bernard.pdf>

BESSONE M., GIACOBBE G., *Il diritto alla riservatezza in Italia e in Francia: due esperienze a confronto*, Padova, 1988

BIANCA C.M., BUSNELLI F.D. (a cura di), *La protezione dei dati personali. Commentario al d.lgs. 30 giugno 2003, n. 196 ("Codice Privacy")*, Padova, 2007

BIASIOTTI A., *Codice della privacy e misure minime di sicurezza: d.lgs. 196/2003*, II ed., Roma, 2004

BIGLIAZZI GERI L., *Procura (dir. priv.)*, in *Enc. dir*., XXXVI, Milano, 1987

BIONDINI P., *Approcci definitori alla "norma tecnica"*, in N. GRECO (a cura di), *Crisi del diritto, tecnica in campo ambientale*, Roma, 1999, 31

BLAIOTTA R., *Appunti sul dolo alla luce della recente giurisprudenza di legittimità sul reato di omissione di referto* (Nota a Cass., sez. fer., 8 settembre 1998, Messori), in *Cass. pen.*, 2000, 1242

BOMBARDELLI M., *Amministrazione digitale*, in *Il diritto-Encicl. giur*., Milano, 2007, vol. I, 382

BOMBARDELLI M., *Informatica pubblica, e-government e sviluppo sostenibile*, in *Riv. it. dir. pubbl. comunitario*, 2002, 991

BOSSI O., *La ricetta medica dopo il d.lgs. n. 178 del 1991*, in *Rass. dir. farmaceutico*, 1992, 373

BRADNBURN N.M., *Medical Privacy and Research*, 30 *The Journal of Legal Studies* 687 (2001)

BREGMAN-ESCHET Y., *Genetic Databases and Biobanks: Who Controls our Genetic Privacy?*, 23 *Santa Clara Computer & High Tech. L.J.* 1 (2006)

BRENNA E., *La valutazione economica delle tecnologie in sanità con particolare riferimento all'area della telemedicina*, in *Sanità pubbl.*, 2001, 89

BROWNSWORD R., *Consent in Data Protection Law: Privacy, Fair Processing and Confidentiality,* in S. GUTWIRTH, Y. POULLET, P. DE HERT, C. DE TERWANGNE, S. NOUWT (a cura di), *Reinventing Data Protection?,* Dordrecht, 2009, 83

BRUSCO A., *Il mondo della salute. Le sfide dell'umanizzazione*, 2003, in Rete: <http://www.sentieriformativi.it/articolo.asp?id=2#_ftnref16>

BRUSCO A., *Umanità per gli ospedali,* Bresso di Bedero, 1983

BUCCI O., *La cartella clinica. Profili strumentali, gestionali, giuridici ed archivistici*, Santarcangelo di Romagna, 1999

BUCCOLIERO L., CACCIA C., NASI G., *e-he@lth. Percorsi di implementazione dei sistemi informativi in sanità*, Milano, 2005

BUTTARELLI G., *Banche dati e tutela della riservatezza. La privacy nella Società dell'Informazione*, Milano, 1997

BUZZI F., SCLAVI C., *La cartella clinica: atto pubblico, scrittura privata o "tertium genus"?*, in *Riv. it. medicina legale*, 1997, 1161

BYGRAVE L.A., *Data Protection Law. Approaching Its Rationale, Logic and Limits*, The Hague-London-New York, 2002

BYNUM W.F., *Science and the Practice of Medicine in the Nineteenth Century*, Cambridge, 1994

CACCIA C., *Management dei sistemi informativi in sanità*, Milano, 2008

CAGGIA F., *Il trattamento dei dati sulla salute, con particolare riferimento all'ambito sanitario*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *Il codice del trattamento dei dati personali*, Torino, 2007, 405

CAJANI F., *Alla ricerca del log (perduto)*. Nota a Trib. Chieti sez. pen. 30 maggio 2006, n. 139, in *Diritto dell'Internet*, 2006, 573

CAMMARATA M., MACCARONE E.*, La firma digitale sicura*, Milano, 2003

CANGELOSI G., *I servizi pubblici sanitari: prospettive e problematiche della telemedicina*, in *Dir. famiglia*, 2007, 431

CAPARRELLI P., *Forma volontaria e forma della procura*, in *Giur. it*., 1975, I, 1, 1155

CAPLAN L., *Consent and Anonymization in Research involving Biobanks,* in *Embo Reports,* 2006, Vol. 7, No. 7, 661

CARDARELLI F., SICA S., ZENO-ZENCOVICH V. (a cura di), *Il codice dei dati personali. Temi e problemi*, Milano, 2004

CARLONI E., *Codice dell'amministrazione digitale - Commento al d.lgs. 7 marzo 2005 n. 82*, Rimini, 2005

CARNEVALI U., *Mandato (diritto civile),* in *Encicl. giur. Treccani*, Roma, 1990, vol. XIX

CARTABIA M., *Le norme sulla privacy come osservatorio sulle tendenze attuali delle fonti del diritto*, in M.G. LOSANO (a cura di), *La legge italiana sulla privacy. Un bilancio dei primi cinque anni*, Roma-Bari, 2001, 61

CARTER J.H., *Electronic Health Records. A Guide for Clinicians and Administrators*, II ed., American College of Physicians – Philadelphia, 2008

CASINI M., SARTEA C., *La consulenza genetica in Italia: problemi, regole d consenso informato, trattamento dei dati genetici e privacy*, in *Medicina e morale*, 2009, 1121

CASO R., *Digital rights management: il commercio delle informazioni digitali tra contratto e diritto d'autore*, Padova, 2004, in Rete: <http://eprints.biblio.unitn.it/archive /00001336/>

CASO R., *Un "rapporto di minoranza": elogio dell'insicurezza informatica e della fallibilità del diritto. Note a margine del Trusted Computing*, in R. CASO (a cura di), *Sicurezza informatica: regole e prassi*. Atti del Convegno tenuto presso la Facoltà di Giurisprudenza di Trento il 6 maggio 2005, Trento, 2006, 4

CASONATO C., *Diritto alla riservatezza e trattamenti sanitari obbligatori: un'indagine comparata*, Trento, 1995

CASONATO C., *Il consenso informato. Profili di diritto comparato,* in C. CASONATO, T.E. FROSINI, T. GROPPI (a cura di), *Diritto pubblico comparato ed europeo*, 2009, 1052

CASONATO C., PICIOCCHI C., VERONESI P. (a cura di), *Forum BioDiritto - I dati genetici nel biodiritto*, Padova, in corso di pubblicazione

CASSANO G., FADDA S. (a cura di), *Codice in materia di protezione dei dati personali. Commento articolo per articolo al testo unico sulla privacy d.lgs. 30 giugno 2003, n. 196*, Milano, 2004

CASSANO G., GIANDOMENICO M. (a cura di), *I contratti di intermediazione - Mandato, agenzia, mediazione, contratto estimatorio, commissione, procacciamento d'affari, concessione di vendita, franchising, intermediazione finanziaria*, Padova, 2009

CASSANO G., GIURDANELLA C. (a cura di), *Il codice della pubblica amministrazione digitale - Commentario al d.lgs. n. 82 del 7 marzo 2005*, Milano, 2005

CAVAGNOLI S., IORIATTI FERRARI E., *Tradurre il diritto. Nozioni di diritto e di linguistica giuridica*, Padova, 2009

CHEN C., GARRIDO D., OKAWA G., LIANG L., *The Kaiser Permanente Electronic Health Record: Transforming and Streamlining Modalities of Care*, 28 *Health Affairs* 323 (2009)

CIAN G., *L'intervento di un nuncius nella formazione delle fattispecie negoziali*, in *Studium iuris*, 1996, 13

CIATTI A., *La protezione dei dati idonei a rivelare lo stato di salute nella legge n. 675/1996*, in *Contratto e impr./Europa*, 1998, 368

CIPRIANO G., *La cartella clinica digitale*, in *Dir. sanitario moderno*, 2008, fasc. 1, 17

CORALES M., EGERMANN E., FORGÒ N., KRÜGEL T., *Intellectual Property Rights in E-health: Balancing out the Interests at Stake – a Herculean Task?*, 3 *Int. J. Private Law* 286 (2010)

CORASANITI G., *Esperienza giuridica e sicurezza informatica*, Milano, 2003

CORASANITI G., *La sicurezza dei dati personali*, in F. CARDARELLI, S. SICA, V. ZENO-ZENCOVICH (a cura di), *Il codice dei dati personali. Temi e problemi*, Milano, 2004, 112

CORONATO S., *La documentazione sanitaria in ospedale*, in *Ragiusan*, fasc. 267/268, 2006, 24

CORONATO S., *La tutela della privacy in ospedale*, in *Ragiusan*, 2006, fasc. 265/266, 6

COSENTINI L., *La relazione medico-paziente: rapporto tra dovere di cura e autodeterminazione della persona destinataria della cura. Indisponibilità del diritto alla salute*. Nota a Decr. Trib. Modena 14 maggio 2009, in *Giur. mer.*, 2009, 2697

COSSU U., *Nuncius*, in *Digesto civ.*, Torino, 1995, vol. XII, 3

CRIGGER B.J., *e-Medicine: Policy to Shape the Future of Health Care*, 36 *The Hastings Center Report* 12 (2006)

CUFFARO V., D'ORAZIO R., RICCIUTO V. (a cura di), *Il codice del trattamento dei dati personali*, Torino, 2007

CUSHMAN R., *PHRs and the Next HIPAA*, 2008, in Rete: <http://www.projecthealthdesign.org/media/file/PHR_HIPAA2.pdf>

CUSHMAN R., *Primer: Authentication of identity (with application to PHRs/PHAs)*, in Rete: <http://www.projecthealthdesign.org/media/file/primer_authentication.pdf>

CUSHMAN R., *Primer: Data Protection and the Personal Health Record*, Project Health Design ELSI Team, University of Miami, in Rete: <http://www.projecthealthdesign.org/media/file/primer_data_protection.pdf>

D'ATRI A., SACCA D. (a cura di), *Information Systems: People, Organizations, Institutions, and Technologies*, Heidelberg-Dordrecht-London-New York, 2010

D'AVACK L., *Ordine giuridico e ordine tecnologico*, Torino, 1998

D'AVANZO W., voce *Rappresentanza*, in *Nov. Dig. it*., Torino, 1967, 801

D'ELIA I., PIETRANGELO M., *Il Codice dell'amministrazione digitale nel processo di semplificazione normativa: genesi e criticità*, in *Informatica e dir*., 2005, 9

D'ORAZIO R., *Il principio di necessità nel trattamento dei dati personali*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *Il codice del trattamento dei dati personali*, Torino, 2007, 20

DE AZEVEDO CUNHA M.V., DONEDA D., ANDRADE N., *La re-identificazione dei dati anonimi e il trattamento dei dati personali per ulteriore finalità: sfide alla privacy*, in *Ciberspazio e dir*., 2011, 641

DE CAMELIS P., *Privacy e potere informatico - Cenni al trattamento dei dati inerenti la salute*, in *Rass. amm. sanità*, 1998, 4

DE GIOVANNI E., *Il "Codice dell'amministrazione digitale": prime impressioni*, in *Dir. dell'Internet*, 2005, 226

DE LORENZI V., *La rappresentanza diretta volontaria. Problemi e soluzioni alla luce dell'analisi economica del diritto*, in *Contr. impr*., 1997, 595

DE LORENZI V., *Procura*, in *Digesto civ*., Torino, 1997, vol. XV, 317

DE NARDIS L., *e-Governance Policies for Interoperability and Open Standards*, Yale Information Society Project Working Paper, June - 2010, in Rete: <http://ssrn.com/abstract=1629833>

DE PIETRO O., *Il sanitario ed il referto - Rilievi giuridici e medico legali*, Napoli, 1981

DE VALLES A., *Norme giuridiche e norme tecniche*, in *Scritti in onore di Jemolo*, Milano, vol. III, 1963, 177

DEMUYNCK L., DE DECKER B., *Privacy-Preserving Electronic Health Records*, in J. DITTMANN, S. KATZENBEISSER, A. UHL (a cura di), *Communications and Multimedia Security*. 9th IFIP TC-6 TC-11 Conference, CMS 2005 Salzburg, Austria, September 2005 Proceedings, Laxemburg, Austria, 2005, 150

DEN BESTEN M., *The Rise of Bionformatics*, Working Paper Series, aprile 2003, in Rete: <http://ssrn.com/abstract=1521649>

DI CIOMMO F., *Il trattamento dei dati sanitari tra interessi individuali e collettivi*, in *Danno e resp*., 2002, 121

DI CIOMMO F., *La privacy sanitaria*, in R. PARDOLESI (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Milano, 2003, 239

DI COCCO C., *Soggetti che effettuano il trattamento (Parte I - Titolo IV)*, in J. MONDUCCI, G. SARTOR (a cura di), *Il codice in materia di protezione dei dati personali*, Padova, 2004, 119

DI GREGORIO V., *Rappresentanza legale*, in *Digesto civ*., Torino, XVI, 293

DICK R.S., STEEN E.B., *The Computer-based Patient Record: An Essential Technology for Health Care*, Washington, DC, 1991

DOMMERING E., *Regulating technology: code is not law*, in E. DOMMERING, L. ASSCHER (a cura di), *Coding Regulation. Essays on the Normative Role of Information Technology*, The Hague, 2006, 1

E-HEALTH ERA, *Fact sheet France*, marzo 2007, in Rete: <http://www.ehealth-era.org/database/documents/factsheets/France.pdf>

E-HEALTH ERA, *Fact sheets: England*, marzo 2007, in Rete: <http://www.ehealth-era.org/database/documents/factsheets/UK_England.pdf>

EHR IMPLEMENT, *National policies for EHR implementation in the European area: social and organizational issues. Results of a European Survey*, 30 marzo 2010, in Rete: <http://www.ehr-implement.eu/download.cfm?downloadfile=FD55D882-1143-DEB7-74CEB2C507FFBE3D&typename=dmFile&fieldname=filename>

EHR IMPLEMENT, *WP5 - National reports of EHR implementation - England*, 31 marzo 2008, in Rete: <http://www.ehr-implement.eu/download.cfm?downloadfile=305DE7DF-1143-DEB7-748EFE58B8FA6D90&typename=dmFile&fieldname=filename>

EHR IMPLEMENT, *WP5 – National reports of EHR implementation – France*, 28 maggio 2009, in Rete: <http://www.ehr-implement.eu/download.cfm?downloadfile=A684205D-1143-DEB7-74D3FF51299F09E6&typename=dmFile&fieldname=filename>

EHRLICH I., POSNER R.A., *An Economic Analysis of Legal Rulemaking*, 3 *J. Legal Stud.* 257 (1974)

ELLI G., *Privacy e sicurezza dei dati*, Milano, 2001

ELLUL J., *Il sistema tecnico. La gabbia delle società contemporanee*, Milano, 2009 (trad. it. di G. CARBONELLI; titolo originale: *Le Système technicien*, 1977)

ERCOLANO C., *Codice dell'amministrazione digitale*, in *Nuovo dir.*, 2005, 554

EUSER, *eHealth Country Brief: France*, 2005, in Rete: <http://www.euser-eu.org/eUSER_eHealthCountryBrief.asp?CaseID=2220&CaseTitleID=1061&MenuID=118>

EUSER, *eHealth Country Brief: United Kingdom*, 2005, in Rete: <http://www.euser-eu.org/eUSER_eHealthCountryBrief.asp?CaseID=2228&CaseTitleID=1069&MenuID=118>

EYSENBACH G., *What is e-health? [editorial]*, in *Journal of Medical Internet Research*, vol. 3, n. 2, 2001, e(20)

FABBRI A., MARAN F., *Diritto di accesso e diritto di riservatezza: convivenza possibile?*, in *Ragiusan*, 2006, fasc. 265/266, 10

FADINI U., *Norma e mondo nell'era della tecnica*, in *Dem. dir*., 1987, 25

FAGNIEZ P.L., *Le masquage d'information par le patient dans son DMP, Rapport au ministre de la santé et des solidarités*, 30 janvier 2007, in Rete: <http://www.sante.gouv.fr/htm/actu/fagniez_dmp/rapport.pdf>

FERRAJOLI L., *La sovranità nel mondo moderno. Nascita e crisi dello Stato nazionale*, Roma-Bari, 1997

FERRARI F., *Il codice dell'amministrazione digitale e le norme dedicate al documento informatico*, in *Riv. dir. proc*., 2007, 415

FERRARI F., *La nuova disciplina del documento informatico*, in *Riv. dir. proc*., 1999, 129

FINESCHI V. (a cura di), *Il codice di deontologia medica*, Milano, 1996

FINESCHI V., TURILLAZZI E., *Automatismo o discrezionalità nella trasmissione del referto medico: quale risposta dalla recente giurisprudenza?*, in *Riv. it. medicina legale*, 2002, 291

FINOCCHIARO G., *Il trattamento dei dati sanitari: alcune riflessioni critiche a dieci anni dall'entrata in vigore del Codice in materia di protezione dei dati personali*, in G.F. FERRARI (a cura di), *La legge sulla privacy dieci anni dopo*, Milano, 2008, 207

FINOCCHIARO G., *La firma sul referto di laboratorio*, in *Sanità pubbl. e privata*, 2009, fasc. 3, 5

FIORANELLI M., ZULLINO P., *Io, Ippocrate di Kos*, Roma-Bari, 2009

FIORAVANTI L., *Referto (omissione di)*, in *Digesto pen*., Torino, 1997, vol. XII, 21

FIORI A., LA MONACA G., *Le regole doverose di condotta nel rilascio della ricetta medica* (Nota a Trib. Milano, 25 giugno 1997), in *Riv. it. medicina legale*, 1999, 325

FISICHELLA D., *L'altro potere - Tecnocrazia e gruppi di pressione*, Roma-Bari, 1997

FLORIO A., *Il trattamento dei "dati idonei a rivelare lo stato di salute" da parte dei medici liberi professionisti*, in *Ciberspazio e dir*., 2010, 111

FRÈ F., *La cartella clinica nel sistema sanitario italiano*, in *Nuova rass. legislazione, dottrina e giurisprudenza*, 2007, fasc. 23-24, 2387

FRIEDMAN B., KHAN P.H., BORINING A., *Value Sensitive Design: Theory and Methods*, Technical Report, December 2002, in Rete <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.11.8020&rep=rep1&type=pdf>

FROOMKIN A.M., *ELSI Guide to Licensing Project HealthDesign Work Product in the Public Interest*, *Project HealthDesign*, 2007, in Rete <http://www.projecthealthdesign.org/media/file/ELSI-OpenSource Guide.pdf>

FROOMKIN A.M., *Forced Sharing of Patient-Controlled Health Records*, Working Paper, 2008, in Rete: <http://www.projecthealthdesign.org/media/file/Forced-sharing.pdf>

FROOMKIN A.M., *The New Health Information Architecture: Coping with he Privacy Implications of the Personal Health Records Revolution*, UM ELSI Group for Project HealthDesign, 2008, in Rete: <http://www.projecthealthdesign.org/media/file/social-life-info-15.pdf>

GABRIELLI U., *La cartella clinica ospedaliera*, in *Riv. it. diritto sociale*, 1970, 498

GADAMER H. G., *Dove si nasconde la salute*, Milano, 1994

GAGNEUX M., *Pour un dossier Patient virtule et partagé et une stregie nationale des systèmes d'information de santé*, 23 aprile 2008, in Rete: <http://www.d-m-p.org/docs/Rapport_DMP_mission_Gagneux .pdf>

GALIMBERTI U., *Psiche e techne. L'uomo nell'era della tecnica*, Milano, 1999

GAMBARO A., *Comprendere le strategie comunicative del legislatore*, in *Riv. crit. dir. priv*., 2000, 605

GAMBARO A., SACCO R., *Sistemi giuridici comparati*, II ed., Torino, 2003

GARRI F., *I soggetti che effettuano il trattamento: il titolare, il responsabile e l'incaricato*, in G. SANTANIELLO (a cura di), *La protezione dei dati personali*, in G. SANTANIELLO (diretto da), *Trattato di diritto amministrativo*, vol. XXXVI, Padova, 2005, 131

GARTEE R., *Electronic Health Records. Understanding and Using Computerized Medical Records*, Upper Saddle River - New Jersey, 2007

GASSER U., PALFREY J., *Born Digital - Connecting with a Global Generation of Digital Natives*, Cambridge, MA, 2008

GENTILI A., *Documento informatico e tutela dell'affidamento*, in *Riv. dir. civ*., 1998, fasc. 3, 2, 163

GHERARDI S., STRATI A., *La telemedicina*, Roma, 2004

GIGANTE M., *Alcune osservazioni sull'evoluzione dell'uso del concetto di tecnica*, in *Giur. cost*., 1997, 647

GIGANTE M., *Effetti giuridici nel rapporto tra tecnica e diritto: il caso delle norme «armonizzate»*, in *Riv. it. dir. pubbl. com*., 1997, 313

GIORGINI P., MASSACCI F., ZANNONE N., *Security and Trust Requirements Engineering*, in *FOSAD*, 2005, 237

GIUSTI G., *La figura giuridica del "nunzio"*, in *Nuovo dir*., 1986, 417

GODARD B., SCHMIDTKE J., CASSIMAN J.J., AYMÉ S., *Data storage and DNA banking for biomedical research: informed consent, confidentiality, quality issues, ownership, return of benefits. A professional perspective,* in *European Journal of Human Genetic*s, 2003, vol. 11, suppl. 2, S88

GOLLMAN D., *Computer Security*, III ed., Chichester, 2006

GOOD B.J., *Medicine, Rationality and Experience: An Anthropological Perspective*, Cambridge, 1994

GOODMAN K.W., *Etica, informatica e medicina. L'informatica e la trasformazione dell'assistenza sanitaria*, Roma, 1999 (titolo originale: *Etchics, computing, and medicine: informatics and the transformation of health care*, Cambridge, 1998, trad. it. di E. SANTORO)

GOSTIN L.O., *Health Information Privacy*, 80 *Cornell L. Rev*. 451 (1995)

GOSTIN L.O., HODGE J.G. JR., *Personal Privacy and Common Goods: A Framework for Balancing Under the National Health Information Privacy Rule*, 86 *Minn. L. Rev*. 1439 (2002)

GRAZIADEI M., *Mandato in diritto comparato*, in *Digesto civ*., Torino, 1994, vol. XI, 192

GRAZIADEI M., *Mandato*, in *Digesto civ*., Torino, 1994, vol. XI, 154

GRAZIADEI M., *Mandato*, in *Riv. dir. civ*., 1997, II, 147

GRAZIOSI A., *La nuova efficacia probatoria del documento informatico*, in *Riv. trim. dir. proc. civ*., 2003, 53

GREELY H.T., *Trusted Systems and Medical Records: Lowering Expectations*, 52 *Stan. L. Rev*. 1585 (2000)

GREEN A.J., *Chains of Trust and Duty in Health Information Management*, in *Studies in Ethics, Law, and Technology*, 2009, vol. 3, Issue 1, art. 7

GRIMM D., *Il futuro della Costituzione*, in G. ZAGREBELSKY, P.P. PORTINAIO, J. LUTHER (a cura di), *Il futuro della Costituzione*, Torino, 1996, 129

GRISBY J., KAHENY M.M., SANDBERG E.J., SCHLENKER R.E., SHAUGHNESSY P.W., *Effects and Effectiveness of Telemedicine*, 17 *Health Care Financing Rev.* 115 (1995)

GRITTI F., *La responsabilità civile nel trattamento dei dati personali*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *Il codice del trattamento dei dati personali*, Torino, 2007, 107

GUARDA P., *Agenti software e sicurezza informatica*, in G. PASCUZZI (a cura di), *Diritto e tecnologie evolute del commercio elettronico*, Padova, 2004, 315 (in Rete <http://eprints.biblio.unitn.it/archive /00001424/>)

GUARDA P., *Alla ricerca della sicurezza: società, regole e tecnologia*, in R. CASO (a cura di), *Sicurezza informatica: regole e prassi.* Atti del Convegno tenuto presso la Facoltà di Giurisprudenza di Trento il 6 maggio 2005, Trento, 2006, 129 (in Rete: <http://eprints. biblio.unitn.it/archive/00001136/>)

GUARDA P., *Data Protection, Information Privacy, and Security Measures: an Essay on the European and the Italian Legal Frameworks*, in *Ciberspazio e dir*., 2008, 65 (in Rete: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1517449>)

GUARDA P., *Electronic Health Records: Privacy and Security Issues in a Comparative Perspective*, Working Paper Series, December 26, 2009, in Rete: <http://ssrn.com/abstract=1528461>

GUARDA P., *Fascicolo sanitario elettronico* [aggiornamento-2011], in *Digesto civ*., Torino, in corso di pubblicazione

GUARDA P., MASSACCI F., ZANNONE N., *E-Government and on-line Services: Security and Legal Patterns*, in F. CORRADINI, A. POLZONETTI (eds.), *MeTTeG07*. Proceedings of the 1st International Conference on Methodologies, Technologies and

Tools Enabling e-Government, Camerino, Italy, 27-28 September 2007, 29

GUARDA P., ZANNONE N., *Towards the Development of Privacy-Aware Systems*, in *Information and Software Technology*, vol. 51, 2009, 337

GUERNELLI M., *Riflessi civilistici del "Codice dell'amministrazione digitale"*, *Studium iuris*, 2006, 787

GUERNELLI M., *Il "Codice dell'amministrazione digitale" modificato*, in *Studium iuris*, 2006, 1399

GUERRINI L., *Prime osservazioni in margine alla nuova legge francese sulla protezione dei dati personali*, in *Dir. informazione e informatica*, 2004, 645

HALL M.A., *Property, Privacy and the Pursuit of Integrated Electronic Medical Records*, Wake Forest Univ. Legal Studies Paper No. 1334963, in Rete: <http://ssrn.com/abstract=1334963>

HATCH M., *HIPAA: Commercial Interests Win Round Two*, 86 *Minn. L. Rev.* 1515 (2002)

HAVEMAN H., FLIM C., *eHealth strategy and implementation activities in the Netherlands. Report in the framework of the eHealth ERA project*, E-Health ERA, October 2007, in Rete: <http://www.ehealth-era.org/database/documents/ERA_Reports/eHealth-ERA_Report_Netherlands_03-10-07_final.pdf>

HÄYRY M., CHADWICK R., ÁRNASON V., ÁRNASON G. (a cura di), *The Ethics and Governance of Human Genetic Databases, European Perspectives,* Cambridge, 2007

HELGESSON G., JOHNSSON L., *The Right to Withdraw Consent to Research on Biobank Samples,* in *Medicine, Health Care and Philosophy,* 2005, Vol. 8, No. 3, 315

HERRING S.C., *Questioning the Generational Divide: Technological Exoticism and Adult Constructions of Online Youth Identity*, in D. BUCKINGAM (a cura di), *Youth, Identity, and Digital Media*, The

John D. and Catherine T. MacArthur Foundation Series on Digital Media and Learning, The Mit Press, Cambridge, MA, 2008, 71, in Rete <http://www.mitpressjournals.org/doi/abs/10.1162/dmal.9780262524834.071>

HODGE J.G. ET AL., *Legal Issues Concerning Electronic Health Information: Privacy, Quality, and Liability*, 282 *JAMA* 1466 (1999)

HOFFMAN S., PODGURSKI A., *E-Health Hazards: Provider Liability and Electronic Health Record Systems*, 24 *Berkeley Tech. L.J.* 1523 (2009)

HOFFMAN S., PODGURSKI A., *In Sickness, Health, and Cyberspace: Protecting the Security of Electronic Private Health Information*, Working Paper 06-15, September 2006, in Rete: <http://ssrn.com/abstract=931069>

HOFFMAN S., PODGURSKI A., *Meaningful use and certification of health information technology: what about safety?*, *in Journal of Law, Medicine and Ethics, Forthcoming. Case Legal Studies*, Research Paper No. 2010-34, October 2010, in Rete: <http://ssrn.com/abstract=1697587>

HOFFMAN S., PODGURSKI A., *Securing the HIPAA Security Rule*, Case Research Paper Series in Legal Studies, Working Paper 06-26, December 2006, in Rete: <http://ssrn.com/abstract=953670>

HOLMES S., SUNSTEIN C.R., *Il costo dei diritti. Perché la libertà dipende dalle tasse*, Bologna, 2000

HOWARDS J., STRAUSS A., *Humanizing Health Care,* New York, 1997

HUTTON E., BARRY D., *Medical: Privacy Year in Review: Developments in HIPAA*, 2 *ISJLP* 347 (2006)

ILLICH I., *Nemesi medica. L'espropriazione della salute,* Milano, 1977

IORIATTI FERRARI E. (a cura di), *La traduzione del diritto comunitario ed europeo: riflessioni metodologiche*. Atti del Convegno tenuto presso la Facoltà di Giurisprudenza di Trento 10-11 marzo 2006, Trento, 2007

IPPOCRATE, *Antica Medicina. Giuramento del medico*, a cura di M. VEGETTI, Milano, 1998

IRTI N., SEVERINO E., *Le domande del giurista e le risposte del filosofo (un dialogo su diritto e tecnica)*, in *Contr. e impr*., 2000, 665

IZZO U., GUARDA P., *Sanità elettronica, tutela dei dati personali e digital divide generazionale: ruolo e criticità giuridica della delega alla gestione dei servizi di sanità elettronica da parte dell'interessato*, in *Trento Law and Technology Research Group Research Papers*, n. 3, 2010, in Rete: <http://eprints.biblio.unitn.it/archive/00001921/>

IZZO U., *Medicina e diritto nell'era digitale: i problemi giuridici della cyber medicina*, in *Danno e resp*., 2000, 807

JACOBSON P.D., *Medical Records and HIPAA: Is It Too Late to Protect Privacy?*, 86 *Minn. L. Rev.* 1497 (2002)

JOHNSTON D. ET AL., *The Value of Computerized Provider Order Entry in Ambulatory Settings: Executive Preview*, Wellesley, MA, 2003

JONES V., JOLLIES C., *eHealth strategy and implementation activities in England*, Report in the framework of the eHealth ERA project, 7 June 2007, in Rete: <http://www.ehealth-era.org/database/documents/ERA_Reports/England_eHealth_ERA_Country_Report_final_07-06-2007.pdf>

JORI A., *Medicina e medici nell'antica Grecia: saggio sul Perì tècnes ippocratico*, Bologna, 1996

JÜRJENS J., *Secure Systems Development with UML*, Heidelberg, 2004

JUSO R., *Dati sensibili e consenso informato: profili costituzionali e legislativi*, in *Ragiusan*, 2004, fasc. 247/248, 6

KAGAMI M., TSUJI M., GIOVANNETTI E. (a cura di), *Information Technology Policy and the Digital Divide: Lessons for Developing Countries*, Edward Elgar, Cheltenham, 2004

KAHN R., *Kaiser Permanente Completes Electronic Health Record Implementation*, 2010, in Rete: <http://xnet.kp.org/newscenter/pressreleases/nat/2010/030310ehrcomplete.html>

KAYE J., STRANGER M. (a cura di), *Principles and Practice in Biobank Governance*, Farnham UK - Burlington USA, 2009

KAYE J., STRANGER M., *Governing Biobanks: An Introduction,* in J. KAYE, M. STRANGER (a cura di), *Principles and Practice in Biobank Governance,* Farnham UK - Burlington USA, 2009, 3

KOOPS B.-J., LEENES R., *'Code' and the slow erosion of privacy*, 12 *Mich. Telecomm. Tech. L. Rev.* 115 (2005)

KRUM W.L., LATSHAW J.D., *Training*, in J. WALKER, E.J. BIEBER, F. RICHARDS (a cura di), *Implementing an Electronic Health Record System*, New York, N.Y., 2006, 60

LAMBO L., *La disciplina del trattamento dei dati personali: profili esegetici e comparatistici delle definizioni*, in R. PARDOLESI (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Milano, 2003, 59

LATIFI R. (a cura di), *Current principles and practices of telemedicine and e-health*, Amsterdam, 2008

LAZZARI C., *La guida in stato di ebbrezza tra modalità di accertamento del tasso alcolemico e il reato di omissione di referto ai sensi dell'art. 365 c.p.* (Nota a Giudice di pace Terni, 4 marzo 2003, Paolantoni), in *Rass. giur. umbra*, 2003, 217

LESSIG L., *Code and other Laws of Cyberspace*, New York, 1999

LESSIG L., *Code v. 2*.0, New York, 2006 (in Rete: <http://codev2.cc/>)

LINDER J.A., MA J., BATES D.W., MIDDLETON B., STAFFORD R.S., *Electronic Health Record Use and the Quality of Ambulatory Care in the United States*, 167 *Arch. Intern. Med.* 1400 (2007)

LIPARI N., *Il diritto privato tra fonti statali e legislazione regionale*, in *Giur. it*., 2003, 3

LIPARI N., *Le fonti del diritto*, Milano, 2008

LLOYD I.J., *Information technology law*, V ed., Oxford, 2008

LORD D.B., *The HIPAA Privacy Rule and Medical Records Discovery (part two)*, 30 *AK Bar Rag* 6 (2006)

LOSANO M.G. (a cura di), *La legge italiana sulla privacy. Un bilancio dei primi cinque anni*, Roma-Bari, 2001

LUCIANI M., *L'antisovrano e la crisi delle Costituzioni*, in *Riv. dir. cost*., 1996, 731

LUGARESI N., *Protezione della privacy e protezione dei dati personali: i limiti dell'approccio comunitario*, in *Giust. amm*., 2004, 289

LUPARIA L., ZICCARDI G., *Investigazione penale e tecnologia informatica, L'accertamento del reato tra progresso scientifico e garanzie fondamentali*, Milano, 2007

LUPO N., *Le fonti normative della privacy*, *tra esigenze di aggiornamento e ricerca di stabilità*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *Il codice del trattamento dei dati personali*, Torino, 2007, 777

MACCARI A., ROMIGI G., *Le basi concettuali e pratiche di un Sistema Informativo Sanitario*, Santarcangelo di Romagna, 2009

MACILOTTI M., *Biobanche* [aggiornamento-2011], in *Digesto civ*., Torino, in corso di pubblicazione

MACILOTTI M., *Consenso informato e biobanche di ricerca*, in *Nuova giur. civ.*, 2009, II, 153

MACILOTTI M., IZZO U., PASCUZZI G., BARBARESCHI M., *La disciplina giuridica delle biobanche*, in *Pathologica*, 2008, fasc. 100, 86

MACILOTTI M., *Proprietà, Informazione ed interessi nella disciplina delle biobanche a fini di ricerca*, in *Nuova giur. civ*, 2008, II, 222

MAGLIO M., *Le misure di sicurezza nei sistemi informativi: il punto di vista di un giurista alla luce della legge sulla tutela informatica*, in *Contratto e imp*., 2000, 1

MAGLIONA B., *Documentazione sanitaria (conservazione e archiviazione),* in *Digesto pen.*, Torino, 1990, vol. IV, 169

MALIAPEN M., *Clinical Genomic Data Use: Protecting Patients Privacy Rights*, in *Studies in Ethics, Law, and Technology*, 2009, vol. 3, Issue 1, art. 1

MANETTI M., *Poteri neutrali e Costituzione*, Milano, 1994

MARAN F., FABBRI A., *Il codice per la protezione dei dati personali e l'attività socio-sanitaria integrata*, in *Ragiusan*, 2005, fasc. 257/258, 19

MARGRET M.K., *Electronic Health Records. A Practical Guide for Professionals and Organizations*, Chicago, IL, 2009

MARTINES M., *La protezione degli individui rispetto al trattamento automatizzato dei dati nel diritto dell'Unione europea*, in *Riv. it. dir. pubbl. com*., 2000, 719

MASCHIO F., *Il trattamento dei dati sanitari. Regole generali e particolari trattamenti per finalità di rilevante interesse pubblico*, in *Ragiusan*, 2005, fasc. 257/258, 6

MASCHIO F., *Il trattamento dei dati sanitari. Regole generali e particolari trattamento per finalità di rilevante interesse pubblico*, in G. SANTANIELLO (a cura di), *La protezione dei dati personali*, in G. SANTANIELLO (diretto da), *Trattato di diritto amministrativo*, vol. XXXVI, Padova, 2005, 485

MASSACCI F., MYLOPOULOS J., ZANNONE N., *An Ontology for Secure Socio-Technical Systems*, in *Handbook of Ontologies for Business Interaction*. The IDEA Group, 2007, in Rete: <http://security1.win.tue.nl/~zannone/publication/mass-mylo-zann-07-IDEA.pdf>

MASSACCI F., PREST M., ZANNONE N., *Using a Security Requirements Engineering Methodology in Practice: the compliance with the Italian Data Protection Legislation*, in *Computer Standards & Interfaces*, 2005, 27(5), 445

MASSACCI F., ZANNONE N., *Detecting Conflicts between Functional and Security Requirements with Secure Tropos: John Rusnak and the Allied Irish Bank*, Technical Report DIT-06-002, University of

Trento, 2006, in Rete: <http://security1.win.tue.nl/~zannone/publication/gior-mass-mylo-zann-06-RE.pdf>

MAY C., ELLIS N.T., *When Protocols Fail: Technical Evaluation, Biomedical Knowledge, and the Social Production of 'Facts' about a Telemedicine Clinic*, in *Social Science and Medicine*, vol. 53, Issue 8, 2001, 989

MAZOUÈ J.G., *Diagnosis Without Doctors*, 15 *Med. & Phi*. 559 (1990)

MCCUBBIN C.N., *Legal and Ethico-legal Issues in E-healthcare Research Projects in the UK*, 62 *Social Science & Medicine* 2768 (2006)

MELCHIONNA S., *I principi generali*, in R. ACCIAI (a cura di), *Il diritto alla protezione dei dati personali. La disciplina sulla privacy alla luce del nuovo Codice*, Santarcangelo di Romagna, 2004, 29

MENGONI L., *Diritto e tecnica*, in *Riv. trim. dir. e proc*., 2001, 1

MILLER R.A., *Why the Standard View is Standard: People, not Machines, Understand Patients' Problems*, 15 *J. Med., & Phi* 581 (1990)

MINELLA T., *Privacy e sanità*, in *Ragiusan*, 2005, fasc. 259/260, 22

MINGHETTI P., SANFILIPPO L., *Formalismi nella redazione e nella documentazione della spedizione delle ricette mediche non ripetibili*, in *Ragiufarm*, 1994, fasc. 19, 4

MONDUCCI J., PASETTI G., *Il trattamento dei dati sanitari e genetici (Parte II – Titolo V)*, in J. MONDUCCI, G. SARTOR (a cura di), *Il codice in materia di protezione dei dati personali. Commentario sistematico al d.lgs. 30 giugno 2003, n. 196*, Padova, 2004, 255

MONDUCCI J., SARTOR G. (a cura di), *Il codice in materia di protezione dei dati personali*, Padova, 2004

MONTI A., *Bioinformatica e diritto d'autore. La conoscenza ha bisogno di codici aperti*, in *Ciberspazio e dir*., 2006, 511

MORTON J., *Data Protection and Privacy*, 18 *European Intellectual Property Review* 558 (1996)

MORUZZI M., *Fascicolo Sanitario Elettronico personale e reti e-Health. Appunti per un'analisi della sanità di Internet*, in *Salute e società*, 2008, fasc. 3, 1

MORUZZI M., *Internet e Sanità. Organizzazioni e management al tempo della rete*, Milano, 2008

MOSCO L., *La rappresentanza volontaria nel diritto privato*, Napoli, 1960

MOSCON V., *Rappresentazione informatica dei diritti tra contratto e diritto d'autore*, in *Ciberspazio e dir.*, 2010, 587 (in Rete: <http://eprints.biblio.unitn.it/archive/00001930>)

NARDONE A., TRIASSI M., *Profili organizzativi e giuridici della telemedicina nel quadro delle risorse tecnologiche in sanità*, in *Sanità pubblica e privata*, 2003, 27

NATOLI U., *Rappresentanza (dir. civ.)*, in *Enc. dir.*, XXVIII, Milano, 1987

NELSON L.J., *A Tale of Three Systems: a Comparative Overview of Health Care Reform in England, Canada, and The United States*, 37 *Cumb. L. Rev.* 513 (2006/2007)

NICHOLSON L., *Electronic Health Records in the United Kingdom of Great Britain & Northern Ireland*, in Rete: <http://www.ifhro.org/docs/ElectronicHealthRecordsinUKFINAL.doc>

NIH NATIONAL CENTER FOR RESEARCH RESOURCES, MITRE CORPORATION, *Electronic Health Records Overview*, aprile 2006, in Rete: <http://www.ncrr.nih.gov/publications/informatics/EHR.pdf>

NONIS M., CORVINO G., FORTINO A., *La scheda di dimissione ospedaliera. Manuale pratico di compilazione ed uso dello strumento informativo per la classificazione dei ricoveri per DRG/ROD*, Roma, 1997

NORELLI G.A., MENCARELLI A., FRAVOLINI G., MAZZEO E., *L'obbligo di denuncia e di referto nella legislazione e nella prassi sanitaria*, in *Assistenza soc.*, 1995, I, 279

ONIDA T., ROMANI F., SANTORO S., *Agenti elettronici e rappresentanza volontaria nell'ordinamento giuridico italiano*, in *Informatica e dir*., 2003, 197

ORLANDI S., *Gli adempimenti per i titolari dei trattamenti*, in R. ACCIAI (a cura di), *Il diritto alla protezione dei dati personali. La disciplina sulla privacy alla luce del nuovo Codice*, Santarcangelo di Romagna, 2004, 181

PAGNI A., *Dalla condotta medica alla medicina telematica*, Lettura magistrale alle Giornate nazionali di studio in medicina telematica, 8-9-10 aprile 2010, Firenze, in Rete: <http://www.ordinemedicilatina.it/system/files/DALLA+CONDOTTA+MEDICA+ALLA+MEDICINA+TELEMATICA.pdf>

PALLARO P., *Libertà della persona e trattamento dei dati personali nell'Unione europea*, Milano, 2002

PALMIERI A., PARDOLESI R., *Il codice in materia di protezione dei dati personali e l'intangibilità della «privacy» comunitaria*. Nota a sent. Corte di Giustizia delle Comunità Europee 6 novembre 2003, n. causa C-101/01, in *Foro it.*, 2004, IV, 59

PAMOLLI F., SALERNO N.C., *Spesa sanitaria, demografia, istituzioni*, in M. MADIA (a cura di), *Un welfare anziano. Invecchiamento della popolazione o ringiovanimento della società?*, Bologna, 2007, 103

PARDOLESI R. (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Milano, 2003

PARDOLESI R., *Dalla riservatezza alla protezione dei dati personali: una storia di evoluzione e discontinuità*, in R. PARDOLESI (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Milano, 2003, 1

PASCUZZI G., *Il diritto dell'era digitale*, III ed., Bologna, 2010

PASCUZZI G., *Il diritto fra tomi e bit: generi letterari e ipertesti*, Padova, 1997

PASCUZZI G., IZZO U., *Le problematiche giuridiche connesse all'utilizzo delle nuove tecnologie in sanità*, in *Teleformazione e teleconsulto in sanità: verso un management integrato del paziente oncologico*. Atti del convegno "Teleformazione e teleconsulto in sanità", 9 giugno 2000, Trento, 2000, 155 (in Rete: <http://www.pol-it.org/ital/pascuzzi.htm>)

PASCUZZI G., *Tecnologie digitali e regole*, in *Diritto dell'Internet*, 2005, 303

PATRIZIA P., *In tema di rappresentanza legale dei minori*, in *Giur it*., 1989, 1055

PATTI S., *L'efficacia probatoria del documento informatico*, in *Riv. dir. proc*., 2000, 60

PEIGNÉ V., *Il trattamento dei dati sanitari in Italia e Francia tra convergenze e divergenze*, in *Dir. dell'Internet*, 2008, 296

PEIGNÉ V., *Verso il fascicolo sanitario elettronico: presentazione della riforma francese*, in *Dir. dell'Internet*, 2007, 626

PELLEGRINI P., *Trattamenti di dati personali in ambito sanitario*, in G.P. CIRILLO (a cura di), *Il Codice sulla protezione dei dati personali*, Milano, 2004, 325

PERREAU H.-E., *Les droits de la personnalité*, in *Rev. trim. dr. civ*., 1909, 501

PERRI P., *Le misure di sicurezza*, in J. MONDUCCI, G. SARTOR (a cura di), *Il codice in materia di protezione dei dati personali*, Padova, 2004, 137

PIERRE M.C., *New Technology, Old Issues: The All-Digital Hospital and Medical Information Privacy*, 56 *Rutgers L. Rev*. 541 (2004)

PINNA A., *Autodeterminazione e consenso: da regola per i trattamenti sanitari a principio generale*, in *Contratto e imp*., 2006, 598

POISSANT L., PEREIRA J., TAMBYLIN R., KAWASUMI Y., *The Impact of Electronic Health Records on Time Efficiency of Physicians and*

Nurses: A Systematic Review, 12 *Journal of the American Medical Informatics Associations* 505 (2005)

PORTIGLIATTI BARBOS M., *Referto e denuncia*, in *Digesto pen*., Torino, 1997, vol. XII, 37

POZZI A., *Procura*, in *Enc. giur*., XXIV, Roma, 1991

PRADIERI A., *Le norme tecniche nello Stato pluralista e prefederativo*, in *Il diritto dell'economia*, 1996, 251

PRENSKY M., *Digital Natives, Digital Immigrants*, in *On the Horizon*, vol. 9, n. 5, October 2001, in Rete: <http://www.marcprensky.com/writing /Prensky%20-%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part1.pdf>;

PRENSKY M., *Digital Natives, Digital Immigrants*, Part II: *Do They Really* Think *Differently?,* in *On the Horizon*, vol. 9, n. 6, December 2001, in Rete: <http://www.marcprensky.com/writing/Prensky%20-%20Digital %20Natives,%20 Digital%20Immigrants%20-%20Part2.pdf>

PRIMICERIO B., *La cartella clinica e la documentazione sanitaria ad essa collegata: evoluzione, utilizzazione e responsabilità*, in *Il Diritto sanitario moderno*, 2004, 207

PULICE M., *Privacy: fascicolo sanitario elettronico e referti on-line*, in *Il Civilista*, 2010, fasc. 6, 59

RABAZZI C., PERRI P., ZICCARDI G., *La sicurezza informatica e la Privacy*, in G. ZICCARDI (a cura di), *Telematica giuridica. Utilizzo avanzato delle nuove tecnologie da parte del professionista del diritto*, Milano, 2005, 516

REIDENBERG J.R., *'Lex Informatica', The Formulation of Information Policy Rules Through Technology*, 76 *Tech. L. Rev*. 553 (1998)

RESTA G., *Il diritto alla protezione dei dati personali*, in F. CARDARELLI, S. SICA, V. ZENO-ZENCOVICH (a cura di), *Il codice dei dati personali. Temi e problemi*, Milano, 2004, 45

RICCIO G.M., *Privacy e dati sanitari*, in F. CARDARELLI, S. SICA, V. ZENO-ZENCOVICH (a cura di), *Il codice dei dati personali. Temi e problemi*, Milano, 2004, 247

RINGOLD D.J., SANTELL J.P., SCHNEIDER P.J., *ASHP National Survey of Pharmacy Practice in Acute Care Settings: Dispensing and Administration-1999*, 57 *American Journal of Health-System Pharmacy* 1759 (2000)

ROBOTTI E., *Titolo V. Trattamento di dati personali in ambito sanitario*, in G. CASSANO, S. FADDA (a cura di), *Codice in materia di protezione dei dati personali. Commento articolo per articolo al testo unico sulla privacy d.lgs. 30 giugno 2003, n. 196*, Milano, 2004, 434

ROCCHIETTI G., *La documentazione clinica. Compilazione, conservazione, archiviazione, gestione e suo rilascio da parte della direzione sanitaria. Trattamento dei dati sanitari e privacy,* in *Minerva medicolegale*, 2001, fasc. 1, 15

RODEN D.M., PULLEY J.M., BASFORD M.A., BERNARD G.R., CLAYTON E.W., BALSER J.R., MASYS D.R., *Development of a Large-Scale De-Identified DNA Biobank to Enable Personalized Medicine*, in *Clinical Pharmacology and Therapeutics*, vol. 84, 2008, 362

RODOTÀ S., *Intervista su privacy e libertà*, Roma, 2005

RODOTÀ S., *Privacy e costruzione della sfera privata. Ipotesi e prospettive*, in *Politica del dir.*, 1991, 525

RODOTÀ S., *Repertorio di fine secolo*, Roma, 1999, 226

RODOTÀ S., *Tecnologie e diritti*, Bologna, 1995

RODOTÀ S., *Tra diritto e società. Informazioni genetiche e tecniche di tutela*, in *Riv. crit. dir. priv.*, 2000, 571

RODWIN M.A., *Patient Data: Property, Privacy & the Public Interest*, 36 *Am. J. L. and Med.* 586 (2010)

ROKITA K.A., TOPPER J.E., LAMPMAN M.C., YOUNG D.L., *Extending EHR access to patients*, in J. WALKER, E.J. BIEBER, F. RICHARDS (a

cura di), *Implementing an electronic health record system*, New York, N.Y., 2006, 153

ROPPO V., *Diritto privato regionale?*, in *Riv. dir. priv*., 2003, 11

ROPPO V., *Il contratto*, in G. IUDICA, P. ZATTI (a cura di), *Trattato di diritto privato*, Milano, 2001

ROSSATO A., *Diritto e architettura nello spazio digitale: il ruolo del software libero*, Padova, 2006

ROSSI MORI A., CONSORTI F., *Dalla cartella clinica elettronica locale al fascicolo sanitario personale*, 2003, in Rete <http://www.uniroma2.it/didattica/IINFO2/deposito/IINFO2_5.pdf>

ROSSI MORI A., CONSORTI F., NARDI R., RICCI F.L., *Un quadro di riferimento sulle tecnologie dell'informazione nel settore sanitario*, 2002, in Rete: <http://dns2.icar.cnr.it/cannataro/unicz/didattica/medicina/ISEI-MED-II/ModuloReti/Monografie/QuadroRiferimentoInformaticaSanitaria.pdf>

ROSSI MORI A., MACERATINI R., *La cartella clinica elettronica (Electronic Patient Record)*, 2009, in Rete <http://www.softwaremedico.it/documenti/CartellaClinicaElettronica.pdf>

ROSSI MORI A., *Patient Summary e documentazione clinica*, giugno 2007, in Rete: <http://www.sanitaelettronica.cnr.it/lumir_old/rapporti_pdf/pat_sum.pdf>

ROSSI P., *Denuncia o referto: obblighi del medico operante in «struttura pubblica» ed in particolare nell'Inail*, in *Riv. it. medicina legale*, 1997, 917

ROTHSTEIN M., *Currents in Contemporary Ethics: Research Privacy Under HIPAA and the Common Rule*, 33 *J.L. Med. & Ethic* 154 (2005)

SACCO R., *Antropologia giuridica. Contributo ad una macrostoria del diritto*, Bologna, 2007

SACCO R., *Formante*, in *Digesto civ*., Torino, 1992, vol. VIII, 438

SACCO R., *Traduzione giuridica* [aggiornamento-2000], in *Digesto civ*., Torino, 722

SAFFIOTI C., *Il Codice dell'amministrazione digitale è in vigore. Conoscere uno strumento che coinvolge la pubblica amministrazione, i cittadini e le imprese*, in *L'Amministrazione italiana*, 2006, fasc. 6, 887

SALEEM T., *Implementation of HER/EPR in England: a model for developing countries*, in *Journal of Health Informatics in Developing Countries*, 2009 vol. 3, n. 1, 9, in Rete: <http://www.jhidc.org/index.php/jhidc/issue/view6>

SALMONI F., *Le norme tecniche*, Milano, 2001

SALOMONI A., *La rappresentanza volontaria*, in P. CENDON (a cura di), *Contratti*, IX, Torino, 2000, 57

SALZANO G., *I diritti dell'interessato*, in J. MONDUCCI, G. SARTOR (a cura di), *Il codice in materia di protezione dei dati personali. Commentario sistematico al d.lgs. 30 giugno 2003, n. 196*, Padova, 2004, 19

SANTANIELLO G. (a cura di), *La protezione dei dati personali*, in G. SANTANIELLO (diretto da), *Trattato di diritto amministrativo*, vol. XXXVI, Padova, 2005

SANTORO E., *Le cartelle cliniche personali in rete*, Roma, 2008

SANTORO E., *Web 2.0 e Medicina, Come social network, podcast, wiki e blog trasformano la comunicazione, l'assistenza e la formazione in sanità*, Roma, 2009

SARTORETTI C., *Contributo allo studio del diritto alla privacy nell'ordinamento costituzionale. Riflessioni sul modello francese*, Torino, 2008

SARTORI L., *La tutela della salute pubblica nell'Unione europea*, Cittadella, 2009

SARZANA DI S. IPPOLITO C., *La protezione dei dati personali nel campo sanitario: problemi giuridici e tecnologici*, in *Dir. informazione e informatica*, 1999, 29

SARZANA DI S. IPPOLITO C., *Responsabilità penali connesse al trattamento ed all'uso dei dati sanitari*, in *Dir. pen. e proc*., 2002, 903

SCALISI V., *Complessità e sistema delle fonti di diritto privato*, in *Riv. dir. civ*., 2009, 147

SCHMITT C., *L'epoca delle neutralizzazioni e delle politicizzazioni*, in G. MIGLIO, P. SCHIERA (a cura di), *Le categorie del politico*, Bologna, 1972, 179

SCHNEIER B., *Beyond Fear. Thinking Sensibly about Security in an Uncertain World*, New York, NY, 2003

SCHNEIER B., *The Psychology of Security*, 2008, in Rete: <http://www.schneier.com/essay-155.html>

SCHWARTZ P.M., *Privacy and the Economics of Health Care Information*, 76 *Tex. L. Rev*. 1 (1997)

SEVERINO E., *Il destino della tecnica*, Milano, 1998

SFARDINI A., TOSONI P., *Navigare la rete. Per un approccio analitico agli stili di navigazione*, in F. PASQUALI, B. SCIFO (a cura di), *Consumare la rete. La fruizione di internet e la navigazione del web*, Milano, 2004, 121

SGRECCIA E., *Non archiviare l'impegno per l'umanizzazione della medicina,* in *Medicina e Morale*, 1986, fasc. 2, 267

SHORTER E., *La tormentata storia del rapporto medico paziente*, Milano, 1986

SILVESTRI G., *La parabola della sovranità. Ascesa declino e trasfigurazione di un concetto*, in *Riv. dir. cost*., 1996, 3

SIMONCINI A., *Il sistema delle fonti normative*, in V. CUFFARO, V. RICCIUTO (a cura di), *Il trattamento dei dati personali. Vol. II: profili applicativi*, Torino, 1999, 11

SIMONS W.W., MANDL K.D., KOHANE I.S., *The PING Personally Controlled Electronic Medical Record System: Technical Architecture*, 12 *J. Am. Med. Informatics Ass'n* 47 (2005)

SINHA A., *An Overview of Telemedicine: The Virtual Gaze of Health Care in the Next Century*, 14 *Medical Anthropology Quarterly. New Series* 291 (2000)

SKENE L., *Feeding Back Significant Findings to Participants and Relatives*, in J. KAYE, M. STRANGER (a cura di), *Principles and Practice in Biobank Governance*, Farnham UK - Burlington USA, 2009, 161

SOLOVE D.J., *The Digital Person. Technology and Privacy in the Information Age*, New York, 2004

SPANTIGATI F., *Il valore giuridico delle norme tecniche*, in *Jus*, 2001, 279

STALLINGS W., *Network Security Essentials: Applications and Standards*, III ed., Upper Saddle River, New Jersey, 2007

STEIN T. (a cura di), *The Electronic Physician*, Chicago, IL, 2005

STILIO L., *Il diritto all'autodeterminazione informativa: genesi storica di un diritto fondamentale dell'homo tecnologicus*, in *Nuov. dir*., 2002, 19

SWIRE P.P., STEINFELD L.B., *Security and Privacy After September 11: The Health Care Example*, 86 *Minn. L. Rev*. 101 (2002)

TANG P.C., MCDONALD C.J., *Electronic health record systems,* in E.H. SHORTLIFFE, J.J. CIMINO (a cura di), *Biomedical informatics: Computer applications in health care & biomedicine,* New York, NY, 2006, 447

TAYLOR P., *A Survey of Research in Telemedicine*, in *Telemedicine Services. Journal of Telemedicine and Telecare*, 4, 2, 1998, 223

TERRY N.P., *A Medical Ghost in the E-Health Machine*, 14 *Health Matrix* 225-29 (2004)

TERRY N.P., *Certification and Meaningful Use: Reframing Adoption of Electronic Health Records as a Quality Imperative*, in *Indiana Journal of Health Law, Forthcoming. Saint Louis U. Legal Studies.* Research Paper No. 2010-29, October 2010, in Rete: <http://ssrn.com/abstract=1687658>

TERRY N.P., *Electronic health records: International, structural and legal perspectives*, 12 *Journal of Legal Medicine* No. 1 (2004), in Rete: <http://ssrn.com/abstract=1265025>

TERRY N.P., FRANCIS L.P., *Ensuring the Privacy and Confidentiality of Electronic Health Records*, 2007 *U. Ill. L. Rev.* 681 (2007)

TERRY N.P., *Personal Health Records: Directing More Costs and Risks to Consumers?,* Working Paper, 2008, in Rete: <http://ssrn.com/abstract=1248768>

THALER R.H., SUNSTEIN C.R., *Nudge: Improving Decisions About Health, Wealth, and Happiness*, New Haven-London, 2008

TIRALTI M.C., PERIOLI L., AMBROGI V., ROSSI C., *Aspetti normativi della ricetta medica*, in *Rass. dir. farmaceutico*, 2004, 7

TIZIAN M., *Aspetti giuridici dell'acquisizione del referto come notizia di reato*, in *Riv. giur. polizia*, 2005, 679

TIZIAN M., *Obbligo di referto e lesioni personali*, in *Riv. giur. polizia*, 2001, 373

TOSI F., *La tutela della riservatezza nei codici di deontologia professionale del medico e dell'infermiere, privacy e cartella clinica*, in *Sanità pubblica*, 2006, 60

TOVINO S.A., *The Use and Disclosure of Protected Health Information for Research Under the HIPAA Privacy Rule*, 49 *S.D. L. Rev*. 1439 (2002)

TOWNEND D., TAYLOR M.J., WRIGHTS J., WICKINS-DRAZILOVA D., *Privacy Interests in Biobanking: A Preliminary View on a European Perspective*, in J. KAYE, M. STRANGER (a cura di), *Principles and*

Practice in Biobank Governance, Farnham UK – Burlington USA, 2009, 137

TRABUCCHI A., *La rappresentanza*, in *Riv. dir. civ*., 1978, I, 584

TRABUCCHI R., *Prometeo e la sopravvivenza dell'uomo - Tecnica e prassi per il terzo millennio*, Milano, 1998

VACCARO V., *La cartella clinica* (Nota a TAR VE sez. III 7 marzo 2003, n. 1674), in *Trib. am. reg*., 2003, 180

VAN BAARDEWIJK L.J., *Electronic Health Record in the Netherlands: afraid of the Unknown*, 2009, in Rete: <http://ojs.ubvu.vu.nl/alf/article/viewFile/93/158>

VAN KLNIK B.M.J., PRINS J.E.J., *Law and regulation: scenarios for the information age*, Amsterdam, 2002

VARANI E., *Diritto alla privacy e trattamento dei dati sensibili in ambito sanitario: dalla Carta dei diritti fondamentali dell'Unione Europea al d.lgs. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali"*, in *Giur. it.*, 2005, 1769

VARANI E., *Il diritto di accesso ai documenti amministrativi contenenti dati sanitari*, in *Foro amm. - T.A.R*., 2005, 929

VARANO R., *Forma della procura e contratto concluso dal rappresentante*, in *Notariato*, 1998, 116

VESPERTINI G. (a cura di), *L'e-Government*, Milano, 2004

VICIANI S., *Brevi osservazioni sul trattamento dei dati inerenti la salute e la vita sessuale in ambito sanitario*, in *Riv. critica dir. privato*, 2007, 315

VICIANI S., *L'autodeterminazione «informata» del soggetto e gli interessi rilevanti (a proposito dell'informazione sul trattamento sanitario)*, in *Rass. dir. civ*., 1996, 272.

WAEGEMANN C.P., *Status Report 2002: Electronic Health Records*, Medical Record Institute, 2002

WAGNER W.J., *Development of the Theory of the Right to Privacy in France*, 1971 *Wash. U. L. Q*. 45 (1971)

WALKER J., BIEBER E.J., RICHARDS F. (a cura di), *Implementing an electronic health record system*, New York, N.Y., 2006

WHITE T.J., HOFMANN C.A., *The Privacy Standards Under the Health Insurance Portability and Accountability Act*, 106 *W. Va. L. Rev*. 709 (2004)

WILLISON D.J., *Use of Data from the Electronic Health Record for Health Research – current governance challenges and potential approaches*, marzo 2009, in Rete <http://www.priv.gc.ca/information/pub/ehr_200903_e.pdf>

WILSON E.V. (a cura di), *Patient-centered e-health*, Hershey, Pa., New York, N.Y., 2009

WYATT S. ET AL., *The Digital Divide, Health Information and Everyday Life*, 7 *New Media Society* 199 (2005)

WYATT S. ET AL., *They Came, They Surfed, They Went Back to the Beach, Conceptualising Use and Non-use of the Internet*, in S. WOOLGAR (a cura di), *Virtual Society?*, Oxford, 2002, 23

ZAMBRANO V., *Dati sanitari e tutela della sfera privata*, in *Dir. informazione e informatica*, 1999, 1

ZAMPI C.M., BACCI M., BENUCCI G., BALDASSARRI L., *Diritto alla salute, diritto alla privacy e consenso dell'avente diritto*, in *Riv. it. medicina legale*, 2001, 1037

ZANUTTO A., *Innovazione tecnologica e apprendimento organizzativo: la telemedicina e il sapere medico*, Milano, 2008

ZARABZADEH A., BRADLEY R.W.G., GRIMSON J., *Ensuring Participant Privacy in Networked Biobanks*, J. KAYE, M. STRANGER (a cura di), *Principles and Practice in Biobank Governance*, Farnham UK - Burlington USA, 2009, 177

ZICCARDI G., *Crittografia e diritto. Crittografia, utilizzo e disciplina giuridica documento informatico e firma digitale, segretezza delle informazioni e sorveglianza globale*, Torino, 2003

QUADERNI PUBBLICATI NELLA COLLANA DEL DIPARTIMENTO DI SCIENZE GIURIDICHE

1. *Legal Scholarship in Africa* - MARCO GUADAGNI (1989)

2. *L'insegnamento della religione nel Trentino-Alto Adige* - ERMINIA CAMASSA AUREA (1990)

3. *Il nuovo processo penale. Seminari* - MARTA BARGIS (1990)

4. *Proprietà-garanzia e contratto. Formule e regole nel leasing finanziario* - MAURO BUSSANI (1992)

5. *Fonti e modelli nel diritto dell'Europa orientale* - GIANMARIA AJANI (1993)

6. *Il giudizio di "congruità" del rapporto di cambio nella fusione* - LUIGI ARTURO BIANCHI (1993)

7. *Interessi pubblici e situazioni soggettive nella disciplina della concorrenza del mercato* - FRANCO PELLIZZER (1993)

8. *La legge controllata. Contributo allo studio del procedimento di controllo preventivo delle leggi regionali* - EMANUELE ROSSI (1993)

9. *L'oggetto del giudizio sui conflitti di attribuzione tra i poteri dello Stato. Fonti normative. Strumenti e tecniche di giudizio della Corte Costituzionale* - DAMIANO FLORENZANO (1994)

10. *Dall'organizzazione allo sviluppo* - SILVIO GOGLIO (1994)

11. *Diritto alla riservatezza e trattamenti sanitari obbligatori: un'indagine comparata* - CARLO CASONATO (1995)

12. *Lezioni di diritto del lavoro tedesco* - ULRICH ZACHERT (1995)

13. *Diritti nell'interesse altrui. Undisclosed agency e trust nell'esperienza giuridica inglese* - MICHELE GRAZIADEI (1995)

14. *La struttura istituzionale del nuovo diritto comune europeo: competizione e circolazione dei modelli giuridici* - LUISA ANTONIOLLI DEFLORIAN (1996)

15. *L'eccezione di illegittimità del provvedimento amministrativo. Un'indagine comparata* - BARBARA MARCHETTI (1996)

16. *Le pari opportunità nella rappresentanza politica e nell'accesso al lavoro. I sistemi di "quote" al vaglio di legittimità* - (a cura di) STEFANIA SCARPONI (1997)

17. *I requisiti delle società abilitate alla revisione legale* - EMANUELE CUSA (1997)

18. *Germania ed Austria: modelli federali e bicamerali a confronto* - FRANCESCO PALERMO (1997)

19. *Minoranze etniche e rappresentanza politica: i modelli statunitense e canadese* - CARLO CASONATO (1998)

20. *Scritti inediti di procedura penale* - NOVELLA GALANTINI e FRANCESCA RUGGIERI (1998)

21. *Il dovere di informazione. Saggio di diritto comparato* - ALBERTO M. MUSY (1999)

22. *L'*Anti-Rousseau *di Filippo Maria Renazzi (1745-1808)* - BEATRICE MASCHIETTO (1999)

23. *Rethinking Water Law. The Italian Case for a Water Code* - NICOLA LUGARESI (2000) (versione digitale disponibile su http://eprints.biblio.unitn.it/)

24. *Making European Law. Essays on the 'Common Core' Project* - MAURO BUSSANI e UGO MATTEI (2000)

25. *Considerazioni in tema di tutela cautelare in materia tributaria* - ALESSANDRA MAGLIARO (2000)

26. *Rudolf B. Schlesinger – Memories* - UGO MATTEI e ANDREA PRADI (2000)

27. *Ordinamento processuale amministrativo tedesco (VwGO)* – Versione italiana con testo a fronte - GIANDOMENICO FALCON e CRISTINA FRAENKEL (cur.) (2000)

28. *La responsabilità civile. Percorsi giurisprudenziali* (Opera ipertestuale. Libro + Cd-Rom) - GIOVANNI PASCUZZI (2001)

29. *La tutela dell'interesse al provvedimento* - GIANDOMENICO FALCON (2001)

30. *L'accesso amministrativo e la tutela della riservatezza* - ANNA SIMONATI (2002)

31. *La pianificazione urbanistica di attuazione: dal piano particolareggiato ai piani operativi* - (a cura di) DARIA DE PRETIS (2002)

32. *Storia, istituzione e diritto in Carlo Antonio de Martini (1726-1800). 2° Colloquio europeo Martini, Trento 18-19 ottobre 2000, Università degli Studi di Trento* - (a cura di) HEINZ BARTA, GÜNTHER PALLAVER, GIOVANNI ROSSI, GIAMPAOLO ZUCCHINI (2002)

33. *Giustino D'Orazio. Antologia di saggi. Contiene l'inedito "Poteri prorogati delle camere e stato di guerra"* - (a cura di) DAMIANO FLORENZANO e ROBERTO D'ORAZIO (2002)

34. *Il principio dell'apparenza giuridica* - ELEONORA RAJNERI (2002)

35. *La testimonianza* de relato *nel processo penale. Un'indagine comparata* - GABRIELLA DI PAOLO (2002)

36. *Funzione della pena e terzietà del giudice nel confronto fra teoria e prassi. Atti della Giornata di studio - Trento, 22 giugno 2000* - (a cura di) MAURIZIO MANZIN (2002)

37. *Ricordi Politici. Le «Proposizioni civili» di Cesare Speciano e il pensiero politico del XVI secolo* - PAOLO CARTA (2003)

38. *Giustizia civile e diritto di cronaca. Atti del seminario di studio tenuto presso la Facoltà di Giurisprudenza dell'Università degli Studi di Trento, 7 marzo 2003* - (a cura di) GIOVANNI PASCUZZI (2003)

39. *La glossa ordinaria al Decreto di Graziano e la glossa di Accursio al Codice di Giustiniano: una ricerca sullo* status *giuridico degli eretici* - RUGGERO MACERATINI (2003)

40. *La disciplina amministrativa e penale degli interventi edilizi. Un bilancio della normativa trentina alla luce del nuovo testo unico sull'edilizia. Atti del Convegno tenuto nella Facoltà di Giurisprudenza di Trento l'8 maggio 2003* - (a cura di) DARIA DE PRETIS e ALESSANDRO MELCHIONDA (2003)

41. *The Protection of Fundamental Rights in Europe: Lessons from Canada* - CARLO CASONATO (ED.) (2004)

42. *Un diritto* per *la scuola. Atti del Convegno* "Questioni giuridiche ed organizzative per la riforma della scuola". Giornata di Studio in onore di Umberto Pototschnig (Trento, 14 maggio 2003). *In appendice: U. Pototschnig, SCRITTI VARI (1967-1991)* - (a cura di) DONATA BORGONOVO RE e FULVIO CORTESE (2004)

43. *Giurisdizione sul silenzio e discrezionalità amministrativa. Germania - Austria - Italia* - CRISTINA FRAENKEL-HAEBERLE (2004)

44. *Il processo di costituzionalizzazione dell'Unione europea. Saggi su valori e prescrittività dell'integrazione costituzionale sovranazionale* - (a cura di) ROBERTO TONIATTI e FRANCESCO PALERMO (2004)

45. *Nuovi poteri del giudice amministrativo e rimedi alternativi al processo. L'esperienza francese* - ANNA SIMONATI (2004)

46. *Profitto illecito e risarcimento del danno* - PAOLO PARDOLESI (2005)

47. *La procreazione medicalmente assistita: ombre e luci* - (a cura di) ERMINIA CAMASSA e CARLO CASONATO (2005)

48. *La clausola generale dell'art. 100 c.p.c. Origini, metamorfosi e nuovi ruoli* - MARINO MARINELLI (2005)

49. *Diritto di cronaca e tutela dell'onore. La riforma della disciplina sulla diffamazione a mezzo stampa. Atti del convegno tenuto presso la Facoltà di Giurisprudenza dell'Università di Trento il 18 marzo 2005* - (a cura di) ALESSANDRO MELCHIONDA e GIOVANNI PASCUZZI (2005)

50. *L'Italia al Palazzo di Vetro. Aspetti dell'azione diplomatica e della presenza italiana all'ONU* - (a cura di) STEFANO BALDI e GIUSEPPE NESI (2005)

51. *Appalti pubblici e servizi di interesse generale. Atti dei seminari tenuti presso la Facoltà di Giurisprudenza di Trento. Novembre - Dicembre 2004* - (a cura di) GIAN ANTONIO BENACCHIO e DARIA DE PRETIS (2005)

52. *Il termalismo terapeutico nell'Unione europea tra servizi sanitari nazionali e politiche del turismo* - ALCESTE SANTUARI (2006)

53. *La gestione delle farmacie comunali: modelli e problemi giuridici* - (a cura di) DARIA DE PRETIS (2006)

54. *Guida alla ricerca ed alla lettura delle decisioni delle corti statunitensi* - (a cura di) ROBERTO CASO (2006) (versione digitale disponibile su http://eprints.biblio.unitn.it/)

55. *Dialoghi sul danno alla persona.* Saggi raccolti nell'ambito della seconda edizione dei "Dialoghi di diritto civile" tenutisi presso il Dipartimento di Scienze Giuridiche dell'Università di Trento (a.a. 2004-2005) - (a cura di) UMBERTO IZZO (2006)

56. *Il diritto degli OGM tra possibilità e scelta.* Atti del Convegno tenuto presso la Facoltà di Giurisprudenza di Trento. 26 novembre 2004 - (a cura di) CARLO CASONATO e MARCO BERTI (2006)

57. *Introduzione al biodiritto. La bioetica nel diritto costituzionale comparato* - CARLO CASONATO (2006) (versione digitale disponibile su http://eprints.biblio.unitn.it/)

58. *La famiglia senza frontiere.* Atti del convegno tenuto presso la Facoltà di Giurisprudenza dell'Università di Trento il 1° ottobre 2005 - (a cura di) GIOVANNI PASCUZZI (2006)

59. *Sicurezza informatica: regole e prassi.* Atti del Convegno tenuto presso la Facoltà di Giurisprudenza di Trento il 6 maggio 2005 - (a cura di) ROBERTO CASO (2006) (versione digitale disponibile su http://eprints.biblio.unitn.it/)

60. *Attività alberghiera e di trasporto nel pacchetto turistico* all inclusive*: le forme di tutela del turista-consumatore*. Atti del Convegno. Trento-Rovereto, 4-5 novembre 2005 - (a cura di) SILVIO BUSTI e ALCESTE SANTUARI (2006)

61. *La Società Cooperativa Europea. Quali prospettive per la cooperazione italiana?* Atti del Convegno tenuto presso la Facoltà di Economia di Trento il 24 giugno 2005 - (a cura di) ANTONIO FICI e DANILO GALLETTI (2006)

62. *Le impugnazioni delle delibere del c.d.a. Premesse storico-comparatistiche* - SILVANA DALLA BONTÀ (2006)

63. *La traduzione del diritto comunitario ed europeo: riflessioni metodologiche*. Atti del Convegno tenuto presso la Facoltà di Giurisprudenza di Trento, 10-11 marzo 2006 - (a cura di) ELENA IORIATTI FERRARI (2007)

64. *Globalizzazione, responsabilità sociale delle imprese e modelli partecipativi* - (a cura di) STEFANIA SCARPONI (2007)

65. *Il contratto di trasporto di persone marittimo e per acque interne* - ALCESTE SANTUARI (2007)

66. *Il Private enforcement del diritto comunitario della concorrenza: ruolo e competenze dei giudici nazionali.* Atti del Convegno tenuto presso la Facoltà di Giurisprudenza di Trento, 15-16 giugno 2007 - (a cura di) GIAN ANTONIO BENACCHIO e MICHELE CARPAGNANO (2007) (volume non destinato alla vendita; versione digitale disponibile su http://eprints.biblio.unitn.it/)

67. *L'azione di risarcimento del danno per violazione delle regole comunitarie sulla concorrenza* - GIAN ANTONIO BENACCHIO e MICHELE CARPAGNANO (2007) (volume non destinato alla vendita; versione digitale disponibile su http://eprints.biblio.unitn.it/)

68. *Modelli sanzionatori per il contrasto alla criminalità organizzata. Un'analisi di diritto comparato* - (a cura di) GABRIELE FORNASARI (2007)

69. *Il fattore "R". La centralità della riscossione nelle manovre di finanza pubblica. Atti del Convegno. Trento, 17 novembre 2006* - (a cura di) ALESSANDRA MAGLIARO (2007)

70. *Digital Rights Management. Problemi teorici e prospettive applicative.* Atti del Convegno tenuto presso la Facoltà di Giurisprudenza di Trento il 21 ed il 22 marzo 2007 - (a cura di) ROBERTO CASO (2008) (versione digitale disponibile su http://eprints.biblio.unitn.it/)

71. *Il riconoscimento e l'esecuzione della sentenza fallimentare straniera in Italia* - LAURA BACCAGLINI (2008)

72. *Libertà di riunione - Versammlungsfreiheit in Italien* - CLEMENS ARZT (2008)

73. *Diligentia quam in suis* - GIANNI SANTUCCI (2008)

74. *Appalti pubblici e concorrenza: la difficile ricerca di un equilibrio.* Atti dei seminari tenuti presso la Facoltà di Giurisprudenza di Trento Maggio - Giugno 2007 - (a cura di) GIAN ANTONIO BENACCHIO e MICHELE COZZIO (2008)

75. *L'assegno di mantenimento nella separazione. Un saggio tra diritto e scienze cognitive* - CARLO BONA e BARBARA BAZZANELLA (2008)

76. *Bioetica e* confessioni *religiose*. Atti del Convegno tenuto presso la Facoltà di Giurisprudenza di Trento il 12 maggio 2006 - (a cura di) ERMINIA CAMASSA e CARLO CASONATO (2008)

77. *Poteri di autotutela e legittimo affidamento. Il caso tedesco* - CRISTINA FRAENKEL-HAEBERLE (2008)

78. *Problemi attuali della giustizia penale internazionale. Aktuelle Probleme der Internationalen Strafjustiz*. Atti del XXVII Seminario internazionale di studi italo-tedeschi, Merano 26-27 ottobre 2007. Akten des XXVII. Internationalen Seminars deutsch-italienischer Studien, Meran 26.-27. Oktober 2007 - (a cura di / herausgegeben von) GABRIELE FORNASARI e ROBERTO WENIN (2009)

79. *Pubblicazioni scientifiche, diritti d'autore e Open Access.* Atti del Convegno tenuto presso la Facoltà di Giurisprudenza di Trento il 20 giugno 2008 - (a cura di) ROBERTO CASO (2009) (versione digitale disponibile su http://eprints.biblio.unitn.it/)

80. *Il superamento del passato e il superamento del presente.* La punizione delle violazioni sistematiche dei diritti umani nell'esperienza argentina e colombiana - (a cura di) EMANUELA FRONZA e GABRIELE FORNASARI (2009)

81. *Diritto romano e regimi totalitari nel '900 europeo.* Atti del seminario internazionale (Trento, 20-21 ottobre 2006) - (a cura di) MASSIMO MIGLIETTA e GIANNI SANTUCCI (2009)

82. *Pena e misure di sicurezza. Profili concettuali, storici e comparatistici* - JOSÉ LUIS GUZMÁN DALBORA - (edizione italiana a cura di) GABRIELE FORNASARI ed EMANUELE CORN (2009)

83. *Il governo dell'energia tra Stato e Regioni* - (a cura di) DAMIANO FLORENZANO e SANDRO MANICA (2009)

84. *E-learning e sistema delle eccezioni al diritto d'autore* - SIMONETTA VEZZOSO (2009) (versione digitale disponibile su http://eprints.biblio.unitn.it/)

85. *The concept of «subordination» in European and comparative law* - LUCA NOGLER (2009)

86. *Procedimento penale di pace e principi costituzionali.* Atti del Convegno organizzato dalla Regione Autonoma Trentino-Alto Adige e dal Dipartimento di Scienze Giuridiche dell'Università di Trento. Trento, Facoltà di Giurisprudenza, 1 e 2 febbraio 2008 - (a cura di) MARCELLO LUIGI BUSETTO (2009) (volume non destinato alla vendita)

87. *Accesso aperto alla conoscenza scientifica e sistema trentino della ricerca.* Atti del Convegno tenuto presso la Facoltà di Giurisprudenza di Trento il 5 maggio 2009 - (a cura di) ROBERTO CASO e FEDERICO PUPPO (2010) (versione digitale disponibile su http://eprints.biblio.unitn.it/)

88. *Il divieto di macellazione rituale (*Shechità Kosher *e* Halal*) e la libertà religiosa delle minoranze* - PABLO LERNER e ALFREDO MORDECHAI RABELLO (con una presentazione di ROBERTO TONIATTI) (2010)

89. *Il Difensore civico nell'ordinamento italiano. Origine ed evoluzione dell'Istituto* – DONATA BORGONOVO RE (2010)

90. *Verso quale federalismo? La fiscalità nei nuovi assetti istituzionali: analisi e prospettive* - (a cura di) ALESSANDRA MAGLIARO (2010)

91. *«Servius respondit». Studi intorno a metodo e interpretazione nella scuola giuridica serviana – Prolegomena I* – MASSIMO MIGLIETTA (2010) (versione digitale disponibile su http://eprints.biblio.unitn.it/)

92. *Il pluralismo nella transizione costituzionale dei Balcani: diritti e garanzie* – (a cura di) LAURA MONTANARI, ROBERTO TONIATTI, JENS WOELK (2010)

93. *Studi sul contratto estimatorio e sulla permuta nel diritto romano*, ENRICO SCIANDRELLO (2011)

94. *Fascicolo Sanitario Elettronico e protezione dei dati personali*, PAOLO GUARDA (2011) (versione digitale disponibile su http://eprints.biblio.unitn.it/)