Rivista elettronica di Diritto, Economia, Management

Numero 1 - 2010 • Società dell'Informazione (1990-2010)
Peer Review
a cura di Donato A. Limone

FONDATA E DIRETTA DA
DONATO A. LIMONE

CLIOedu®

Direzione e redazione
Via Antonio Canal, 7
00136 Roma
donato.limone@gmail.com

Gli articoli pubblicati nella rivista sono sottoposti ad una procedura di valutazione anonima. Gli articoli sottoposti alla rivista vanno spediti alla sede della redazione e saranno dati in lettura ai referees dei relativi settori scientifico disciplinari.

Anno I, n. 1, dicembre, 2010
ISSN 2039-4926
Autorizzazione del Tribunale civile di Roma N. 329/2010 del 5 agosto 2010
Editor ClioEdu
Roma - Lecce

INDICE

Presentazione della Rivista

La "Rivista elettronica di Diritto, Economia, Management" è un periodico totalmente digitale, accessibile e fruibile gratuitamente sul sito www.giuritecne.it

La rivista ha lo scopo di trattare le diverse tematiche giuridiche, economiche e manageriali, relative a specifici argomenti monografici, con un approccio integrato e trasversale, di tipo comparato, in un contesto locale, nazionale, comunitario ed internazionale caratterizzato dalla società dell'informazione, dalla globalizzazione dei mercati, da processi innovativi di tipo manageriale ed organizzativo.

La rivista ha anche la finalità di ospitare contributi di giovani studiosi che non avrebbero molte opportunità di pubblicare perché fuori da circuiti culturali ed accademici.

Il Fondatore e direttore della Rivista
Donato A. Limone

Editoriale

Questo numero è il *primo* ed unico del primo anno (2010) della *"Rivista elettronica di Diritto, Economia, Management"*.
È totalmente dedicato alla *"Società dell'Informazione"* nei primi suoi 20 anni (1990-2010).
Le tematiche trattate sono di carattere generale (D. Limone, Politica e normativa comunitaria per la Società dell'informazione (1990-2010)); più specificatamente giuridico: sul commercio elettronico a dieci anni dalla direttiva 2000/31 (L. Bugiolacchi); sul diritto dell'informatica e la società dell'informazione (A. Viola); sui reati informatici (P. Galdieri); sulla tutela dei dati personali (S. Di Minco); sul procedimento amministrativo informatico (W. D'Avanzo); sull'egovernment e la società dell'informazione (M. Mancarella). Sul tema piu' generale della innovazione e del cambiamento organizzativo l'articolo di G. Maggiore; su aspetti metodologici e tecnologici relativi all'e-government il contributo di P. L. Di Viggiano. Sulle tematiche connesse alla sanità elettronica due scritti: il primo, di G. Preite, sulle politiche dei servizi sanitari digitali; il secondo, di A. Buscemi, sulle tecnologie per prevenire errori nel settore sanitario. Il numero si chiude con due contributi piu' strettamente legati alle tecnologie: la sicurezza informatica (C. Ciampi); metodologie e tecniche per l'elearning (E. Limone).

Il Direttore
Donato A. Limone

Autori di questo numero

Bugiolacchi Leonardo

Dottore di ricerca in Informatica e diritto dell'informatica presso l'Università "La Sapienza" di Roma, è docente a contratto di Diritto commerciale presso le Facoltà di Giurisprudenza ed Economia dell'Università Telma Sapienza. Avvocato civilista in Roma, si occupa da anni di questioni giuridiche legate alle tecnologie dell'informazione e della comunicazione. Il diritto della responsabilità civile e delle assicurazioni costituiscono l'altra area principale della sua attività professionale. Membro dell'ANDIG (Associazione nazionale di docenti informatica giuridica), fa parte del Comitato di redazione della Rivista "Responsabilità civile e previdenza", per la quale cura anche il Massimario delle assicurazioni e della circolazione stradale. È autore di numerosi saggi e note a sentenza pubblicati sulle più importanti riviste giuridiche.

E-mail: leonardo.bugiolacchi@libero.it; pec: leonardobugiolacchi@ordineavvocatiroma.org

Buscemi Antonino

Ricercatore di diritto dell'Economia presso la Fondazione Formit e docente di Risk Management Sanitario e Tutela dei dati sanitari presso la Libera Università Luspio.

E-mail: buscemi.antonino@virgilio.it

Ciampi Claudia

ICT Security Manager e Consulente in "diritto e tecnologie dell'informazione" ed in "metodologie e sistemi di gestione della sicurezza dell'informazione", ha maturato un'esperienza pluriennale nella gestione integrata delle problematiche connesse al diritto dell'informatica, alla sicurezza dei dati ed alle tecnologie dell'informazione. Ha sviluppato la sua competenza operando su realtà complesse del settore pubblico e privato esercitando la propria professionalità presso le più importanti società internazionali e nazionali di consulenza direzionale, tra le quali Ernst & Young Consultants S. p. A., Cap Gemini Ernst & Young S.p.A. e Key Consultants S.r.l. . Lead Auditor ISO/IEC 27001 è docente su tematiche legate al Diritto dell'Informatica per organizzazioni private e pubbliche e sui temi dell'Information Security Management per Master universitari.

E-mail: claudiaciampi@me.com

D'Avanzo Wanda

Avvocato e dottore di ricerca in Filosofia del diritto presso l'Università degli studi di Napoli Federico II. E' stata docente a contratto di Storia delle dottrine politiche presso l'Università Telematica Unitelma-Sapienza di Roma. Presso la medesima Università, attualmente collabora

con la cattedra di Filosofia del diritto e Informatica giuridica. Ha pubblicato L'e-govenrment, Movimedia, Lecce, 2007 e Partecipazione, democrazia, comunicazione pubblica. Percorsi di innovazione della Pubblica Amministrazione digitale.

E-mail: wanda.davanzo@unitelma.it

Di Minco Sandro

Avvocato in Pescara. Dottore di Ricerca in Informatica giuridica e diritto dell'informatica, Università degli Studi "La Sapienza" di Roma. Professore "J. Monnet" nell'Università degli Studi di Camerino, di Diritto dell'informatica nell'UE, titolare del Modulo europeo "*Globalisation and the community approach for an information society. current general legal framework"*. Docente di Filosofia del diritto e informatica giuridica nell'Università degli Studi "G. D'Annunzio" di Chieti/Pescara (2005-2010). Docente nel Master in Diritto dell'informatica e teoria e tecnica della normazione, Università degli Studi "La Sapienza" di Roma. Ha svolto attività di ricerca e docenza, sin dai primi anni novanta, in Informatica giuridica e in Diritto dell'informatica, sia in ambito universitario (ad es. : Università degli Studi di Camerino, Università degli Studi "La Sapienza" di Roma, Università "Federico II" di Napoli, Università degli Studi "G. D'Annunzio" di Chieti -Pescara, Università degli Studi di Padova, Università degli studi di Lecce, Università LUMSA di Roma, Università Telematica UNITELMA, Università di Montpellier), che in organismi istituzionali di ricerca, in Italia e all'estero (ad es. ha svolto attività di ricerca presso l'IDG del CNR di Firenze – oggi ITTIG – presso l'IRETIJ di Montpellier e presso l'ERCIM del CNRS, sempre di Montpellier). E' stato il primo Professore J. Monnet in Italia ad insegnare la disciplina del "Diritto comunitario dell'informatica e delle nuove tecnologie" a partire dall'A. A. 2000/01 nell'Università di Camerino. Ha pubblicato saggi, articoli e studi inerenti l'Informatica giuridica e il Diritto dell'informatica collaborando con riviste giuridiche nazionali e internazionali. Ha tenuto seminari, conferenze e relazioni - in Italia e all'estero – sulle principali tematiche inerenti i settori disciplinari suddetti. Ha svolto e svolge attività di consulenza legale nei suddetti ambiti occupandosi costantemente della formazione di dirigenti e quadri del settore privato e pubblico.

E-mail: sandro.diminco@tin.it

Di Viggiano Pasquale Luigi

Dottorando di ricerca in Scienze Giuridiche; Docente di *Sanità digitale*, Master in *Management sanitario* - Libera Università LUSPIO - Roma; Iscritto AIS (Sez. Sociologia del diritto)) e socio ANDIG; Componente del Comitato scientifico del LEG (Laboratorio di eGovernment) - Università del Salento; Componente del Centro di Studi sul Rischio, Università del Salento. Autore e curatore di diversi lavori di ricerca sociale e di pubblicazioni in materia di Informatica giuridica: tra cui: *Il rischio del futuro* (Pensa Multimedia, Lecce 2008); *Rapporto tra sostenibilità, turismo e tecnologie (ICT)* (UNI Service, Trento 2008); *L'amministrazione digitale negli Enti locali. I modelli organizzativi e gli strumenti tecnico*-giuridici, Tangram Edizioni Scientifiche, Trento 2009).

E-mail: luigi.diviggiano@gmail.com; PEC: luigi.diviggiano@pec.it

Galdieri Paolo

Avvocato penalista, docente di Diritto Penale dell'Informatica, Facoltà di Giurisprudenza Luiss di Roma. Docente di Diritto Penale e di Diritto Processuale Penale, Università telematica Unitelma-Sapienza di Roma. Nel 2005 ha redatto per conto della Unione Europea un rapporto sulla Legislazione e prassi giudiziaria in materia di reati informatici in Italia. Ha partecipato a numerosi convegni nazionali e internazionali, tra i quali quello tenuto a Quito in Ecuador e a Dubai negli Emirati Arabi. Autore di numerose pubblicazioni, tra cui le monografie *Teoria e pratica nell'interpretazione del reato informatico,* Giuffrè, Milano, 1997; *Sicurezza e privacy in azienda. Gli aspetti tecnici, psicologici e giuridici*, Apogeo, Milano, 2001; *Cyberterrorismo. L'impiego delle reti telematiche da parte del terrorismo internazionale*, Jackson libri, Milano, 2002.

E-mail: paolo.galdieri@tiscali.it

Limone Donato

Ordinario di Informatica giuridica e docente di Scienza dell'Amministrazione digitale, Università telematica Unitelma-Sapienza, Roma; Presidente dell'Associazione Nazionale Docenti di Informatica Giuridica (Andig); Direttore del Laboratorio di eGovernment, Università del Salento.

E-mail: donato.limone@gmail.com

Limone Edoardo

Ha conseguito la laurea in Comunicazione d'Impresa Marketing e Pubblicità e la laurea specialistica in Marketing e Comunicazione d'Impresa. Attualmente, presso la Fondazione Formit, è consulente per la ricerca, la progettazione ed il monitoraggio di soluzioni ICT presso lo Stato Maggiore Difesa e le Forze Armate. In tale ambito ha offerto supporto su tematiche come ad esempio l'e-learning con un progetto finalizzato a rendere interoperabili le piattaforme di formazione militari a livello mondiale. La virtualizzazione dei sistemi della Difesa e l'introduzione della SOA, partecipando attivamente allo sviluppo dei vari progetti. È nel Gruppo di Lavoro per il progetto DII per la creazione di una rete militare unica ed integrata. In passato ha collaborato, sempre in ambito Formit, con altri enti quali il Ministero della Giustizia nel progetto Notizie di Reato 2 e con diverse Pubbliche Amministrazioni nel processo di censimento, razionalizzazione e reingegnerizzazione dei processi lavorativi (Provincia di Viterbo; Comune di Trieste; comune di S. Vito dei Normanni).

E-mail: elimone@gmail.com

Maggiore Giulio

Ricercatore di Economia e gestione delle imprese presso la Facoltà di Giurisprudenza dell'università telematica Unitelma Sapienza, dove ricopre anche l'incarico di Direttore del master universitario di primo livello in *Management e funzioni di coordinamento delle professioni sanitarie*. Svolge attività di ricerca sui temi della strategie d'impresa, del marketing esperienziale, dell'in-

novazione, delle reti interorganizzative, in collaborazione con varie strutture, fra cui il l'Istituto di ricerche sulle attività terziarie (IRAT) del CNR, a cui è associato. Ha, inoltre, maturato numerose esperienze di consulenza nei settori del marketing strategico, della comunicazione e dell'information technology.

E-mail: giulio.maggiore@unitelma.it

Mancarella Marco

Professore Aggregato di"Informatica della Pubblica Amministrazione" presso il C. d. L. Triennale in "Scienze politiche e delle Relazioni internazionali", nonchè di "Informatica giuridica" presso il C. d. L. Magistrale in "Scienza della politica" dell'Università del Salento. Direttore del Master in "Management pubblico, eGovernment e Federalismo fiscale" e Vice Direttore del Laboratorio di eGovernment dell'Università del Salento. Socio aggregato ANDIG (Associazione Nazionale Docenti di Informatica Giuridica). Consulente FORMEZ - Dipartimento della Funzione Pubblica - Presidenza del Consiglio dei Ministri. Componente del Consiglio Direttivo dell'Istituto per le Politiche dell'Innovazione. Avvocato amministrativista in Lecce e componente del Direttivo dell'Associazione Italiana dei Giovani Avvocati (AIGA) - Sezione di Lecce. Relatore in numerosi Convegni nazionali sul Diritto Amministrativo Elettronico, DAE Roma e seminari all'estero in tema di Amministrazione Digitale (Università Autonoma di Barcellona, Università Parigi XIII). Visiting Professor negli anni 2009 e 2010 presso l'Università Parigi XIII, ove ha tenuto corsi in tema di eGovernment.

E-mail: marco.mancarella@unisalento.it

Preite Gianpasquale

Docente di Scienza dell'amministrazione digitale nel Corso di Laurea Magistrale in Scienze della Politica (LM-62) ed è Responsabile organizzativo del Laboratorio di ricerca sull'eGovernment, Sezione di Scienze Politiche del Dipartimento FCSF dell'Università del Salento. Svolge attività di ricerca sull'evoluzione delle politiche pubbliche, con particolare riferimento ai seguenti temi: Aritmetica politica e biometria, sicurezza e privacy, politica sanitaria, riforma amministrativa e governo elettronico. È inoltre membro della Società Italiana di Scienza Politica (SISP). Tra le pubblicazioni recenti: *Politica e tecnologie. Spazio pubblico e privato della conoscenza nella società dell'informazione*, Carocci, Roma 2010.

E-mail: gianpasquale.preite@unisalento.it

Viola Angela

Laurea in Giurisprudenza presso l'Università degli Studi di Roma "La Sapienza", dove è stata assistente e cultrice della materia in Filosofia del Diritto dal 1993 al 1996, in Teoria dell'interpretazione dal 1994 al 2010, in Diritto Costituzionale dal 2000 al 2010, in Informatica Giuridica dal 2005 al 2009. Avvocato dal 1997. Dottore di ricerca in Informatica Giuridica

e Diritto dell'Informatica, 1999/2000. Docente al Corso di Perfezionamento in Informatica Giuridica Università degli Studi di Roma "La Sapienza" a. a. 2000/2001; Docente al Master Universitario II° Livello in Diritto e Commercio elettronico Università LUMSA Roma a. a. 2002/2003: "Le comunicazioni commerciali". Docente e Tutor al Master Universitario II° Livello Diritto dell'Informatica e Teoria e Tecnica della Normazione - Università degli Studi di Roma "La Sapienza", dal 2002 al 2010. Docente presso Università Telematica Telma (Unitelma) di diritto commerciale a. a. 2005/2006- 2006/2007 – 2007/2008 Laurea Specialistica Diritto della Società dell'Informazione afferente alla Facoltà di Giurisprudenza. Docente al Master di 1° Livello Diritto e Commercio Elettronico - Università Telematica Telma (Unitelma). Componente ANDIG (Associazione Nazionale Docenti Informatica Giuridica) . Stage c/o School of Law Boston University USA in qualità di visiting research attinente al programma di dottorato di ricerca (1997). Pubblicazioni: "Aspetti etici del concetto di standard giuridico" in Esperienze giuridiche del 900 (a cura di F. Modugno), Giuffrè 2000. Diritto ed Intelligenza artificiale nel pensiero di Vittorio Frosini, In ricordo di Vittorio Frosini, Giuffrè, 2004 (cura di A. Jellamo e F. Riccobono), Giuffrè, 2004. Città metropolitane e Roma Capitale, in Trasformazioni della funzione legislativa. IV. Ancora in tema di fonti del diritto e rapporti Stato - Regione dopo la riforma del Titolo V della Costituzione, a cura di Franco Modugno - Paolo Carnevale - Pubblicazioni del Dipartimento di Scienze Giuridiche Università degli Studi di Roma "la Sapienza", Jovene, 2008.

E-mail: angela.viola@virgilio.it

Rivista elettronica di Diritto, Economia, Management

N. 1 - 2010 · pp. 9-29

Politica e Normativa Comunitaria per la Società della Informazione (1990-2010)

Donato A. Limone

Abstract: Nel 1990 nasce la "Società dell'Informazione" con una politica comunitaria finalizzata alla costituzione delle reti aperte e alla liberalizzazione dei mercati e dei servizi delle telecomunicazioni. Il primo decennio (1990-2000) viene caratterizzato da una politica e da una normativa legata ad esigenze e mercati verticali, senza un approccio unitario e sistematico. Il secondo decennio (2000-2010) si sviluppa nella logica di una politica ed una normativa comunitaria che pongono al centro lo sviluppo delle comunicazioni elettroniche. Si giunge al 2010 (Agenda digitale), tuttavia, con la constatazione di avere mancato un obiettivo di mercato integrato e quindi con la necessità di una svolta politica per un approccio integrato, orizzontale, sistemico con l'obiettivo di creare un mercato interno della società dell'informazione. L'obiettivo per il 2020 è quello di superare la logica di mercati e servizi verticali che non portano valore aggiunto ma seguono logiche che ancora una volta tendono a garantire i singoli Paesi Membri ma non a creare un vero mercato interno del settore.
The "Information Society" started in 1990 with an EEC policy aimed at the establishment of open networks and the liberalization of markets and telecommunications services. The first decade (1990-2000) is characterized a policy and legislation related to the needs of vertical markets, without a unified and systematic approach. The second decade (2000-2010) developed the logic of a EEC policy and a legislation focused on the development of electronic communications. We arrive at 2010 (The Digital Agenda), where it became clear that the objective of integrated markets had failed and the need for a policy shift towards an integrated, horizontal system with the goal of creating an internal market for the information society. The goal for 2020 is to overcome the logic of vertical markets and services
that do not add value. Once again this guarantees individual member countries but that does not create a true internal market in the sector.

Parole chiave: comunicazioni elettroniche; elearning; lavoro; eGovernment; sanità elettronica; accessibilità; e-economia; divario digitale.

Sommario: 1. Premessa – 2. La politica comunitaria per la società dell'informazione – 2.1. Il libro bianco della commissione J. Delors (1993) – 2.2. Il rapporto Bangemann sulla società dell'informazione (1994) – 2.3. Il lavoro nella società dell'informazione – 2.4. Convergenza tra i settori delle telecomunicazioni, dell'audiovisivo e delle tecnologie dell'informazione: Le implicazioni normative – 3. La politica comunitaria

Articolo pervenuto il 5 ottobre 2010, approvato il 20 novembre 2010

per la società dell'informazione (2000-2010) – 3.1. La disabilità: una questione di interesse comunitario – 3.2. La eEconomia e le imprese europee – 3.3. Un pacchetto di direttive CE in materia di comunicazioni elettroniche (2002): verso una nuova politica comunitaria del settore – 3.4. eEurope 2005: una società dell'informazione per tutti – 3.5. L'apprendimento online: programma eLearning (2004-2006) – 3.6. eGovernment: l'amministrazione in linea – 3.7. Verso una economia della conoscenza – 3.8. Riutilizzo dell'informazione del settore pubblico – 3.9. Servizi paneuropei di governo elettronico – 3.10. Una nuova strategia per la società dell'informazione e i media – 3.11. La sanità elettronica – 3.12. Contenuti creativi on line – 3.13. Verso una società dell'informazione accessibile – 3.14. Le tecnologie dell'informazione e della comunicazione per le zone rurali – 3.15. Le tecnologie dell'informazione e della comunicazione (TIC) per l'efficienza energetica – 3.16. Le tecnologie emergenti e future (TEF) in Europa – 3.17. Competenze informatiche per il XXI secolo – 3.18. Una strategia per una crescita intelligente, sostenibile, inclusiva – 3.19. Un'agenda digitale per l'Europa – 4. La normativa europea sulla Società dell'informazione – 5. Considerazioni finali.

1. Premessa

Nel 1985 ho pubblicato il volume *Politica e normativa comunitaria per l'informatica (1974-1984),* Milano, Giuffrè; dopo 25 anni ritorno sull'argomento ma con un approccio integrato che tratta sia l'informatica sia le telecomunicazioni, le comunicazioni elettroniche, il commercio elettronico, le firme elettroniche, ecc., ma anche temi più squisitamente politici come i piani di sviluppo eEurope, la società della informazione, l'economia della società dell'informazione, la società dell'accesso elettronico (eAccessibilità), la inclusione elettronica, l'amministrazione digitale o eGovernment, la sanità elettronica, l'eLearning.

Nel volume del 1985 si faceva riferimento alla politica comunitaria tutta rivolta alla creazione di un mercato informatico della Comunità ma si sottolineava anche l'importanza che si dava alle tecnologie dell'informazione per il passaggio verso una società dell'informazione. Nel documento Davignon del 1979 (*La società europea di fronte alle nuove tecnologie dell'informazione. Per una risposta comunitaria*; COM (79) 650 del 9 novembre 1979) ci sono già le basi della politica comunitaria per la società dell'informazione. Verso questa nuova politica il documento della Commissione *Il lavoro di fronte alle nuove tecnologie della micro-elettronica*, COM (80) 16 del 5 febbraio 1980), avvia una riflessione sistematica su quali azioni mettere in campo per affrontare alcuni temi di politica sociale ed economica (incidenza delle tecnologie dell'informazione sul mondo del lavoro e sull'ambiente sociale), e come definire programmi nei settori vitali dell'istruzione, della formazione e della diffusione delle informazioni. Ma ci si preoccupava anche del rapporto tra formazione professionale e nuove tecnologie (*Formazione professionale e nuove tecnologie: nuove iniziative comunitarie per il periodo 1983-1987*, COM (82) 296 del 3 giugno 1982).

Ma nel decennio 1980-1990 veniva varato il progetto "Esprit" (microelettronica avanzata; tecnologia del software; elaborazione avanzata dell'informazione; l'automazione degli uffici; la fabbricazione integrata con il calcolatore; il sistema di scambio delle informazioni); ma si

affrontava il problema della tutela dei diritti individuali rispetto all'uso sempre piu' diffuso di banche dati personali; prendeva corpo una politica di normalizzazione dei contratti pubblici nel settore dell'informatica.
Nel quinquennio 1985-1990 la politica comunitaria matura un percorso che porterà alla definizione di una politica comunitaria per la società dell'informazione e quindi alla formazione di una normativa di supporto così importante da determinare la legislazione dei singoli Paesi Membri della Comunità.
La politica e la normativa comunitaria della società dell'informazione trovano la loro genesi in due direttive: la direttiva 387/90 in tema di "reti aperte"; la direttiva 388/90 in materia di mercati e servizi dell'informazione. Con queste direttive si supera definitivamente il piano comunitario (e anche l'illusione) per un mercato comunitario dell'informatica in concorrenza con quello americano e si sposta l'attenzione verso l'uso di tecnologie per le telecomunicazioni e per i mercati ed i servizi delle stesse telecomunicazioni, quindi verso un mercato dell'informazione. Siamo in piena nuova politica che non si occupa quasi esclusivamente di tecnologie ma di mercati e servizi in termini di concorrenza.
Con il documento Bangemann del 1994 si inaugura la politica comunitaria in materia di "Società dell'informazione". Noi ci occuperemo di analizzare la evoluzione della politica e della normativa di questa "Società": nella quale viviamo, operiamo; con la quale dobbiamo confrontarci di continuo in quanto il paradigma della società dell'informazione ancora non è stato assimilato pienamente (siamo troppo legati alle tecnologie e all'uso delle stesse).

2. La politica comunitaria per la Società dell'informazione (1990-2000)

Nel 1987 viene pubblicato il *"Libro verde sullo sviluppo del marcato comune per i servizi e le apparecchiature di telecomunicazioni"* con la finalità di varare la politica comunitaria in materia di telecomunicazioni con tre obiettivi fondamentali:

a) Liberalizzare i segmenti di mercato ancora in regime di monopolio;
b) Armonizzare il settore delle telecomunicazioni in Europa mediante norme e standard comuni;
c) Applicare con rigore le norme sulla concorrenza ai segmenti di mercato liberalizzati per evitare accordi collusivi e l'abuso o la costituzione di posizioni dominanti.

Le due direttive richiamate 90/387 (Le reti aperte di telecomunicazioni) e 90/388 (Liberalizzazione del mercato dei servizi delle telecomunicazioni) costituiscono la base normativa sulla quale si è sviluppata la politica comunitaria in materia di tecnologie e servizi per la società dell'informazione.

2.1. Il Libro Bianco della commissione J. Delors (1993)

Nel Libro Bianco *"Crescita, competitività e occupazione – Le sfide e le vie da percorrere per entrare nel XXI secolo" (COM (93) 700, Commissione Europea sotto la guida di Jacques Delors, 1993)* si delineavano le direttrici della politica comunitaria piu' generale in materia di sviluppo, competitività e mercato del lavoro rispetto ad un nuovo contesto socio-politico-economico europeo ed internazionale. Il Libro Bianco definiva tre elementi fondamentali per lo sviluppo:

- Un quadro macroeconomico in grado di sostenere le forze di mercato e non di ostacolarle come in passato;
- Interventi di carattere strutturale volti ad accrescere la competitività verso l'esterno del sistema europeo e a permettere di sfruttare tutte le potenzialità del mercato interno;
- Una riforma strutturale del mercato del lavoro per rendere piu' semplice e meno oneroso il ricorso alla manodopera, aumentando così l'intensità occupazionale della crescita.

Per l'implementazione del mercato interno gli obiettivi che il Libro Bianco del 1993 indicava erano:

- Semplificare il contesto normativo e fiscale;
- Facilitare l'attività delle imprese con iniziative volte a garantire il massimo grado di concorrenza e l'accesso al credito privato;
- Aiutare lo sviluppo delle piccole e medie imprese, spina dorsale del sistema economico europeo, tramite la cooperazione e la costruzione di reti;
- Lanciare il piano di realizzazione delle reti trans europee;
- Promuovere una crescita dell'economia sostenibile sia sul piano della stabilità monetaria, che su quello ambientale.

2.2. Il rapporto Bangemann sulla società dell'informazione (1994)

Nel Libro Bianco di Delors veniva delineata per la prima volta una società dell'informazione e contestualmente la Commissione europea insediava un gruppodi esperti che sotto la guida del commissario Martin Bangemann provvedeva a stilare il rapporto *"L'Europa e la società dell'informazione globale"* (vertice di Corfu', 1994). Per la prima volta ed in modo sistematico la Comunità europea metteva le basi per una politica del settore e per la relativa normativa. Al rapporto Bangemann seguì il primo di azione *La via europea verso la società dell'informazione* (adottato il 19 luglio 1994).

Il Rapporto Bangemann ha trattato quattro tematiche di fondo:

- Liberalizzazione delle telecomunicazioni
- Interconnessione delle reti e interoperabilità
- Incremento della domanda di nuovi servizi telematici
- Definizione di regole comuni per i problemi giuridici e tecnici piu' rilevanti (privacy e security).

Il Rapporto definì 10 aree applicative:

1. rete transeuropea delle amministrazioni pubbliche;
2. rete avanzata per le università e i centri di ricerca;
3. rete sanitaria;
4. gestione del traffico stradale;
5. servizi telematici per i paesi dello SME;
6. reti civiche su base locale, regionale, nazionale ed internazionale;
7. gare di appalto elettroniche con rete europea elettronica di assistenza;
8. telelavoro;
9. insegnamento a distanza;
10. controllo del traffico aereo.

Nel vertice di Corfù furono affrontate altre problematiche:

- Quadro regolamentare e giuridico;
- Reti, servizi di base e applicazioni
- Aspetti sociali e culturali
- Creazione di Information Society Project Office per facilitare la cooperazione.

2.3. Il lavoro nella società dell'informazione

Il Libro verde *"Vivere e lavorare nella società dell'informazione"* (COM (96) 389 def.) ha lo scopo di invitare ad un dialogo politico, sociale e civile sui problemi sociali della società della informazione. La società dell'informazione caratterizza un nuovo mondo del lavoro. Di qui, la necessità di incrementare le conoscenze e la consapevolezza di nuove forme di organizzazione del lavoro; di garantire che le PMI traggano tutti i possibili vantaggi dalla società dell'informazione; di modernizzare le istituzioni della vita lavorativa. Con le Tecnologie dell'Informazione e della Comunicazione (TIC) si puo' aumentare la produttività del lavoro ma anche la sicurezza. Il Libro Verde pose alcune sfide da affrontare: impedire le politiche del "ciascun per sé" ; una gestione piu' efficace del processo di trasformazione delle mansioni; risolvere il problema del divario di competenze; aggiornare e migliorare l'istruzione e la formazione per affrontare la rivoluzione delle TIC.

Come vivere nella società dell'informazione e quali politiche pubbliche adottare? Il Libro Verde indica delle sfide da affrontare: ottimizzare il quadro normativo; il rafforzamento delle risorse umane tramite la conoscenza; attribuzione di responsabilità e poteri a livello locale e integrazione della società tramite gli strumenti ed i servizi della società dell'informazione.

La via europea per una società dell'informazione si basa sul modello sociale caratterizzato dalla concorrenza tra le imprese e la solidarietà tra cittadini e gli Stati membri.

La Comunicazione della Commissione (COM (97)390 def. Del 23.7.1997) *sulla dimensione sociale e il mercato del lavoro in relazione alla società dell'informazione – Priorità alla dimensione umana – le fasi successive,* completa quanto scritto nel Libro Verde *"Vivere e lavorare nella società dell'informazione"* . Nella comunicazione la Commissione suggerisce che le politiche pubbliche nell'ambito della società dell'informazione devono avere gli obiettivi fondamentali di:

- Migliorare l'accesso all'informazione
- Migliorare la democrazia e la giustizia sociale

- Promuovere l'occupabilità e l'apprendimento in tutto l'arco della vita
- Rafforzare la capacità dell'economia dell'UE di raggiungere livelli elevati e sostenibili di occupazione e di crescita
- Porre in atto e promuovere le pari opportunità tra gli uomini e le donne
- Promuovere l'inclusione e aiutare le persone che hanno bisogni speciali e le persone cui si presentano poche opportunità a migliorare la loro posizione
- Migliorare la qualità, l'efficienza e l'immagine delle amministrazioni pubbliche.

Nella Comunicazione sono definite una serie di azioni a livello regionale, nazionale, comunitario ed internazionale finalizzate a valorizzare le potenzialità delle TIC nelle politiche occupazionali e sociali.

Lavorare nella società dell'informazione significa garantire flessibilità di lavoro e sicurezza, la protezione dei dati dei lavoratori, la formazione di attività di telelavoro, sanità e sicurezza nel lavoro, i servizi pubblici dell'occupazione.

2.4. Convergenza tra i settori delle telecomunicazioni, dell'audiovisivo e delle tecnologie dell'informazione. Le implicazioni normative

Il "*Libro verde sulla convergenza tra i settori delle telecomunicazioni, dell'audiovisivo e delle tecnologie dell'informazione e sulle sue implicazioni normative. Verso un approccio alla società dell'informazione*" (COM(97)623, Commissione Europea). Si tratta di un Libro verde dedicato alla "convergenza" delle tecnologie che costituisce il valore aggiunto della società dell'informazione con tutte le relative implicazioni socio-economiche. La convergenza porterà alla nascita di nuovi servizi ampliando il mercato globale della informazione. Il Libro verde si occupa della convergenza sotto il profilo tecnologico e del mercato dell'informazione; individua le barriere, esistenti e potenziali, che potrebbero ostacolare gli sviluppi tecnologici e di mercato; fornisce un quadro dettagliato sotto il profilo normativo; e definisce una politica normativa per superare le barriere del settore. Sicuramente il Libro verde costituisce un primo approccio nuovo per una politica europea nel settore delle comunicazioni.

Dal 1990 al 2000 l'Unione Europea delinea una politica per le TIC e la società dell'informazione sulla base di una normazione finalizzata a creare un sistema di reti aperte di telecomunicazioni ed un mercato dei servizi di telecomunicazioni; affronta poi le problematiche piu' squisitamente di tipo socio-economico relativo alla costruzione di una nuova società e di un nuovo mondo del lavoro basato sulle TIC; sulla fine degli anni novanta l'elemento forte della politica europea del settore delle comunicazioni si basa sulla "convergenza" delle tecnologie delle comunicazioni e sulla necessità di eliminare le barriere per sviluppare questa convergenza.

3. La politica comunitaria per la Società dell'informazione (2000-2010)

L'8 dicembre 1999 la Commissione europea lancia l'iniziativa *"eEurope – una società dell'informazione per tutti"*. Con questa iniziativa si apre una nuova fase della politica comunitaria per la società dell'informazione piu' strettamente collegata a temi quali l'accesso, l'e-economia, il nuovo assetto giuridico delle comunicazioni elettroniche, i piani " eEurope".
L'iniziativa politica "eEurope" segna il passaggio verso una politica globale sulla società dell'informazione. Infatti, i principali obiettivi della iniziativa sono:

- Fare in modo che ciascun cittadino, ciascuna abitazione, scuola, impresa e amministrazione entri nell'era digitale e disponga di un collegamento on-line;
- Creare in Europa una cultura di impresa specifica per la società dell'informazione;
- Garantire che l'intero processo di non crei emarginazione ma rafforzi la fiducia dei consumatori e la coesione sociale.

Dieci sono le azioni proposte nella Comunicazione:

- Fare entrare i giovani europei nell'era digitale;
- Accesso piu' economico a internet;
- Accelerare il commercio elettronico;
- Internet ad alta velocità per ricercatori e studenti;
- Tessere intelligenti per un accesso elettronico sicuro;
- Capitale di rischio per le PMI ad alta tecnologia;
- ePartecipazione per i disabili;
- servizi sanitari on-line;
- trasporti intelligenti;
- amministrazioni on-line.

Come si puo' notare c'è un filo che collega il rapporto Bangemann ed il relativo piano di azioni al programma "eEurope" (dal 1994 al 2000).
Il *Piano d'azione "eEurope 2002". Una società dell'informazione per tutti* (Piano d'azione preparato dal Consiglio e dalla Commissione europea per il Consiglio europeo di Feira, 19-20 giugno 2000). Con il Piano d'azione la Commissione europea adotta una politica di lungo termine e proattiva nel settore della società dell'informazione a livello globale, promuovendo in particolare l'approccio europeo in sedi come il G8, l'OCSE, l'OMC.
Il "Piano di azione eEurope 2002" comprende le linee di sviluppo della politica comunitaria sulla società dell'informazione che saranno oggetto dei successivi interventi in tutto il decennio 2000-2010.

3.1. La disabilità: una questione di interesse comunitario

Nella comunicazione della Commissione al Consiglio, al Parlamento europeo, al comitato economico e sociale e al comitato delle Regioni (COM (2000)284 def.) *"Verso un'Europa senza ostacoli per i disabili"*

Il problema della disabilità viene considerato sotto i diversi aspetti: la mobilità intesa come componente della cittadinanza; verso una maggiore accessibilità; mettere la società dell'informazione a servizio di tutti (progetto eEurope e disabili); proteggere i diritti e gli interessi dei consumatori disabili sul mercato.

3.2. La e-Economia e le imprese europee

Con la comunicazione della Commissione COM (2001) 711 def. del 29.11.2001 *"Effetti dell'e-Economia sulle imprese europee: analisi economica ed implicazioni politiche"* sono presi in esame gli aspetti macroeconomici e microeconomici dell'e-Economia. Quanto ai primi la comunicazione rileva che nella crescita economica dell'Europa è determinante il ruolo delle TIC, anche per quanto riguarda la produttività e l'aumento della occupazione. Gli aspetti microeconomici presi in considerazione sono tanti: la e-economia come catalizzatore del cambiamento; la demografia delle imprese in rapido aumento; il ruolo del capitolo di rischio e del finanziamento sul mercato che caratterizza la dinamica delle imprese; le nuove competenze nelle TIC che per una economia in rapida trasformazione; nuovi modelli d'impresa per l'e-economia; nuovi canali di distribuzione e nuove dinamiche di mercato; mercati elettronici; B2C: un nuovo rapporto tra imprese e consumatori; il ruolo della logistica in termini di sostenibilità; la dimensione mobile: una opportunità strategica per l'Europa. In questo quadro di e-Economia le conseguenze per le politiche delle imprese sono diverse: promozione della piena partecipazione delle PMI alla e-Economia; garantire competenze adeguate per la e-Economia; massimizzare le opportunità offerte dal mercato interno; promuovere l'apertura e la concorrenza; promuovere la ricerca in e-economia; aumentare l'efficienza nei rapporti governo-imprese.

3.3. Un pacchetto di Direttive CE in materia di comunicazioni elettroniche (2002): verso una nuova politica comunitaria del settore

Il pacchetto delle Direttive CE costituisce un capitolo importante della politica e della normativa comunitaria in materia di comunicazione elettronica (mercati, servizi, tecnologie): si sposta il problema dalle tecnologie alle comunicazioni con un cambio "culturale" molto forte; si disciplinano quindi in "modo sistematico" e nuovo l'accesso alle reti di comunicazione elettronica, le autorizzazioni, il servizio universale, la protezione dei dati personali nelle comunicazioni elettroniche.
La "direttiva quadro" (2002/21/CE del 7 marzo 2002) ha lo scopo (assieme alle altre quattro direttive, 19, 20, 22, 58/2002) di rendere il settore delle comunicazioni elettroniche più concorrenziale. Questo pacchetto sarà poi modificato nel 2009 dalle direttive "Legiferare meglio" e "Diritto dei cittadini" nonché dalla creazione di un organismo dei regolatori europei delle comunicazioni elettroniche (BEREC). La direttiva quadro quindi non si

limita a disciplinare le reti e i servizi di telecomunicazioni, ma copre tutte le reti e i servizi di comunicazione elettronica (telefonia vocale fissa, le comunicazioni mobili a larga banda, la televisione via cavo e satellitare. La delibera disciplina la materia relativa alle Autorità nazionali di regolamentazione (Obblighi e funzioni generali; funzioni particolari: gestione delle radiofrequenze; numerazione, assegnazione dei nomi di dominio e indirizzamento; diritti di passaggio; coubicazione e condivisione di elementi della rete e risorse correlate per i fornitori di reti di comunicazione elettronica; sicurezza ed integrità delle reti e dei servizi. La direttiva sabilisce controlli regolamentari delle imprese con potere sul mercato (procedura per l'individuazione e la definizione dei mercati; procedura per l'analisi del mercato; normalizzazione; interoperabilità dei servizi di televisione digitale; risoluzione delle controversie; sanzioni). Le direttive successive di modifica sono 2009/136/CE che modifica le direttive 2002/22 e 2002/58. Con il regolamento CE n. 1211/2009 viene istituito l'organismo dei regolatori europei delle comunicazioni elettroniche (BEREC) e l'Ufficio.

La Direttiva 2002/19/CE regolamenta l'accesso alle reti di comunicazione elettronica e alle risorse correlate e all'interconnessione delle medesime (direttiva accesso). La direttiva istituisce un quadro normativo in grado di favorire la realizzazione di una concorrenza sostenibile e di garantire l'interoperabilità dei servizi di comunicazione elettronica. Anche questa direttiva viene modificata nel 2009.

La Direttiva 2002/20/CE regolamenta le autorizzazioni per le reti e i servizi di comunicazione elettronica (direttiva autorizzazioni). L'innovazione principale della direttiva è la sostituzione delle licenze individuali con delle autorizzazioni generali, accanto alle quali sussiste un regime specifico per l'assegnazione delle frequenze e dei numeri. La Direttiva definisce i diritti minimi derivanti dall'0autorizzazione generale, il diritto d'uso delle frequenze radio e dei numeri. La Direttiva stabilisce condizioni apposte all'autorizzazione generale e ai diritti d'uso specifici; procedure per limitare i diritti d'uso delle frequenze radio; diritti amministrativi e contributi.

La Direttiva 2002/22/CE si occupa del servizio universale e dei diritti degli utenti in materia di reti e di servizi di comunicazione elettronica (direttiva servizio universale) per garantire la disponibilità di una serie minima di servizi di buona qualità, accessibili agli utenti a prezzo sostenibile, senza distorsioni della concorrenza. In particolare i servizi sono: fornitura dell'accesso da postazione fissa e fornitura di servizi telefonici; elenco abbonati e servizi di consultazione; telefoni pubblici a pagamento ed altri punti d'accesso ai servizi pubblici di telefonia vocale, misure speciali destinate ai disabili, designazione delle imprese, accessibilità delle tariffe, qualità del servizio, finanziamento degli obblighi di servizio universale. La Direttiva stabilisce anche i diritti degli utenti. La direttiva è stata modificata dalla Direttiva 2009/136/CE.

La Direttiva 2002/58/CE detta norme in materia di trattamento dei dati personali e della tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche). Il fornitore di un servizio di comunicazione elettronica deve salvaguardare la sicurezza dei suoi servizi. La Direttiva si occupa della conservazione dei dati e delle comunicazioni indesiderate (spamming), dei marcatori (cookies) e degli elenchi pubblici. Le modifiche alla direttiva sono state apportate con le direttive 2006/24/CE e 2009/136/CE.

La Direttiva 2002/77/CE si occupa della concorrenza nei mercati delle reti e dei servizi delle comunicazione elettronica. Viene precisato il concetto di comunicazioni elettroniche; sono

soppressi i diritti esclusivi e speciali; la direttiva si occupa di imprese pubbliche verticalmente integrate; di diritti all'uso delle frequenze; dei servizi relativi agli elenchi degli abbonati; tratta degli obblighi del servizio universale; dei satelliti.
Nel dicembre del 2002 viene pubblicata *l'Ottava relazione della Commissione sull'attuazione del quadro normativo per le telecomunicazioni* (COM (2002) 695 def. del 3.12.2002).
Sull'attuazione del quadro normativo per le comunicazioni elettroniche nell'UE la comunicazione della Commissione al Consiglio, al Parlamento europeo, al Comitato economico e sociale europeo e al Comitato delle Regioni (*La regolamentazione e i mercati europei delle comunicazioni elettroniche*, 2003, COM (2003) 715 def. del 19.11.2003) fa il punto della situazione con particolare riferimento alla concorrenza, alla vita privata e al trattamento dei dati personali, ai singoli Paesi Membri. Un ulteriore aggiornamento viene effettuato con la Comunicazione COM(2004) 759 def. del 2.12.2004. L'undicesima relazione su *"La regolamentazione e i mercati europei delle comunicazioni elettroniche 2005"* viene pubblicata con la Comunicazione COM(2006) 68 def. del 20.2.2006.

3.4. eEurope 2005: una società dell'informazione per tutti

Il *Piano d'azione eEurope 2005: una società dell'informazione per tutti* (Comunicazione COM (2002) 263 def. del 28.5.2002) segue il piano di azione "eEurope 2002" che era soprattutto basato sulla estensione della connettività internet in Europa.Il nuovo piano d'azione mira a tradurre questa connettività in un aumento della produttività economica e un miglioramento della qualità e dell'accessibilità dei servizi a profitto di tutti i cittadini europei, sulla base della infrastruttura a banda larga protetta e ampiamente disponibile. Entro il 2005 l'Europa dovrà dotarsi di: moderni servizi pubblici online; e-government (amministrazioni); servizi di e-learning; servizi di e-health (sanità); un ambiente dinamico di e-business.
Tutto il piano si basa sull'uso della banda larga e sulla diffusione delle buone prassi.

3.5. L'apprendimento on line: programma eLearning (2004-2006)

Con la decisione n. 2318/2003/CE del Parlamento europeo e del Consiglio del 5 dicembre 2003 viene adottato un programma pluriennale (2004-2006) per l'effettiva integrazione delle tecnologie dell'informazione e delle comunicazioni (TIC) nei sistemi di istruzione e formazione in Europa (Programma eLearning). Gli obiettivi specifici del programma sono:

- identificare e promuovere i mezzi per utilizzare l'apprendimento on line allo scopo di rafforzare la coesione sociale e lo sviluppo personale, incoraggiare il dialogo interculturale e lottare contro il cosiddetto "divario digitale";
- promuovere e sviluppare l'utilizzo dell'apprendimento on line per attuare il paradigma dell'istruzione e della formazione permanente in Europa;

- sfruttare il potenziale apprendimento on line allo scopo di rafforzare la dimensione europea dell'istruzione;
- favorire una cooperazione piu' strutturata nel settore apprendimento on line tra i vari programmi e strumenti comunitari e le azioni degli Stati membri;
- prevedere meccanismi intesi a migliorare la qualità dei prodotti e dei servizi nonché ad assicurare la loro efficace divulgazione e lo scambio delle buone pratiche.

Le azioni previste:

- la promozione dell'alfabetizzazione digitale;
- la creazione di campus virtuali europei;
- lo sviluppo di gemellaggi elettronici tra istituti scolastico primari e secondari e la promozione delle formazioni destinate ai docenti (e-Twinning);
- l'attuazione di azioni trasversali e del monitoraggio dell'apprendimento on line.

3.6. eGovernment: l'amministrazione in linea

Il ruolo dell'eGovernment per il futuro dell'Europa è il testo della Comunicazione della Commissione al Consiglio, al Parlamento europeo, al comitato economico e sociale e al comitato delle Regioni (COM (2003) 567 def. del 26.9.2003). "Per eGovernment si intende l'uso delle tecnologie dell'informazione e della comunicazione nelle Pubbliche Amministrazioni, coniugato a modifiche organizzative e all'acquisizione di nuove competenze al fine di migliorare i servizi pubblici e i processi democratici e di rafforzare il sostegno alle politiche pubbliche" (definizione tratta dal testo della comunicazione, pag. 8).

Grazie all'eGovernment il settore pubblico puo' mantenere una buona "governante" nella società della conoscenza. Cio' implica:

- un settore pubblico aperto e trasparente;
- un settore pubblico al servizio di tutti;
- un settore pubblico produttivo che valorizzi al massimo il denaro dei contribuenti.

L'eGovernment puo' incidere su di una migliore qualità della vita attraverso servizi piu' veloci ed efficaci; puo' promuovere la competitività in Europa tramite servizi in rete alle imprese; puo' rafforzare la cooperazione amministrativa. Gli interventi da fare quindi riguardano: l'accesso per tutti; la fiducia nei servizi elettronici; migliorare l'uso dell'informazione del settore pubblico; rafforzare il mercato interno e il senso di cittadinanza europea mediante servizi paneuropei; garantire la interoperabilità dei sistemi per i diversi servizi; l'eGovernment non puo' ridursi solo alla introduzione e all'uso delle tecnologie dell'informazione ma l'eGovernment si caratterizza per i profondi cambiamenti organizzativi che produce. I progetti di eGovernment del piano "eEurope 2005" sono richiamati dalla Comunicazione 567/2003. Nell'ambito della iniziativa "i2010" il piano di eGovernment viene ripreso per accelerare lo stesso piano (Comunicazione COM(2006) 173 def.: *"Il piano di azione eGovernment per l'iniziativa i2010: accelerare l'eGovernment in Europa a vantaggio di tutti"*. Le priorità definite sono: accesso per tutti; lotta contro il divario digitale; maggiore efficacia; servizi d'amministrazione in linea di grande impatto; mettere in atto strumenti chiave quali sistemi interoperabili, autenticazione elettronica dei documenti, archiviazione elettronica; rafforzamento della partecipazione al processo decisionale democratico.

3.7. Verso una economia della conoscenza

Con la comunicazione della Commissione dell'11 febbraio 2003 al Consiglio, al Parlamento europeo, al Comitato economico e sociale europeo e al Comitato delle regioni *"Comunicazioni elettroniche: verso l'economia della conoscenza"* (COM (2003) 65 def.) si traccia un bilancio delle principali misure adottate dall'Unione europea nel settore delle comunicazioni elettroniche. Per rafforzare il mercato delle comunicazioni elettroniche è necessario dare attuazione al nuovo assetto normativo delle comunicazioni elettroniche; incentivare l'impiego delle tecnologie della comunicazione elettronica attraverso l'uso della banda larga con il piano "eEurope 2005"; sostenere e rafforzare le attività di ricerca nel settore.

3.8. Riutilizzo dell'informazione del settore pubblico

La Direttiva 2003/98/CE del Parlamento Europeo e del Consiglio del 17 novembre 2003 relativa al riutilizzo dell'informazione del settore pubblico regolamenta il riutilizzo di documenti in possesso degli enti pubblici (ove sia possibile) per fini commerciali e non. La Direttiva considera le richieste di riutilizzo (prescrizioni per il trattamento delle richieste di riutilizzo); le condizioni di riutilizzo (formati disponibili: principi di tariffazione; trasparenza; licenze; modalità pratiche); considera il tutto secondo i principi della non discriminazione e la equità delle transazioni; il divieto di accordi di esclusiva. La Direttiva viene recepita nel nostro Paese con il dlgs n. 36 del 24 gennaio 2006.

3.9. Servizi paneuropei di governo elettronico

La decisione 2004/387/CE del Parlamento europeo riguarda la erogazione interoperabile di servizi paneuropei di governo elettronico alle amministrazioni pubbliche, alle imprese e ai cittadini (IDABC) per il periodo 2005-2009. Il programma (art. 2) si prefigge i seguenti obiettivi:

a) permettere uno scambio efficace e sicuro di informazioni tra le amministrazioni pubbliche a tutti i livelli appropriati, nonché tra tali amministrazioni e le istituzioni comunitarie od eventualmente altre entità;
b) estendere i benefici dello scambio di informazioni di cui alla lettera a) al fine di facilitare l'erogazione di servizi alle imprese e ai cittadini tenendo conto delle loro esigenze;
c) fornire un ausilio al processo di formazione delle decisioni nella Comunità e facilitare la comunicazione tra le istituzioni comunitarie sviluppando il relativo quadro strategico a livello paneuropeo;
d) pervenire all'interoperabilità tra i diversi settori di intervento e al loro interno e, ove opportuno, con le imprese e i cittadini, in particolare sulla base di un quadro europeo di interoperabilità;

e) contribuire agli sforzi delle amministrazioni pubbliche degli Stati membri e della Comunità in termini di semplificazione delle operazioni, accelerazione delle realizzazioni, sicurezza, efficienza, trasparenza, cultura del servizio e rispondenza;
f) promuovere la diffusione delle buone pratiche e incoraggiare lo sviluppo di soluzioni telematiche innovative nelle amministrazioni pubbliche.

Nell'Allegato I sono riportati i progetti di interesse comune che riguardano attività generali, le politiche e le azioni comunitarie, lo scambio di informazioni tra istituzioni, la cooperazione internazionale e altre reti. Nell'Allegati II sono indicate le misure orizzontali: i servizi paneuropei orizzontali delle amministrazioni in rete; i servizi di infrastrutture, le attività strategiche e di sostegno.

3.10. Una nuova strategia per la società dell'informazione e i media

Il nuovo quadro strategico viene definito dalla Comunicazione della Commissione del 1.6.2005 intitolata *"i2010 – Una società europea dell'informazione per la crescita e l'occupazione"* (COM(2005) 229 def.).
Per questa strategia la Commissione ha proposto tre obiettivi prioritari che la politica comunitaria della società dell'informazione e dei media intende raggiungere entro il 2010: la realizzazione di uno spazio unico europeo dell'informazione, il rafforzamento dell'innovazione e degli investimenti nella ricerca sulle tecnologie dell'informazione e della comunicazione (TIC) e la realizzazione di una società dell'informazione e dei media basata sulla inclusione. Per quanto attiene alla creazione di uno spazio unico europeo dell'informazione, la Commissione ha definito 4 specifici obiettivi:

- aumentare la velocità dei servizi in banda larga in Europa;
- incoraggiare i nuovi servizi e i contenuti on-line;
- migliorare le apparecchiature e le piattaforme in grado di "comunicare tra loro" e
- rendere internet piu' sicura nei confronti delle frodi, dei contenuti dannosi e dei problemi tecnologici.

Riguardo all'obiettivo "innovazione e investimento nella ricerca" la comunicazione riporta un elenco sostanzioso di azioni da effettuare relativamente alla ricerca, alla sicurezza, all'applicazione delle tecnologie nelle PMI, al commercio elettronico, a nuove forme di lavoro a sostegno dell'innovazione nelle imprese, ecc.
L'obiettivo "inclusione" comprende una serie di interventi mirati a sostenere e promuovere l'accessibilità elettronica, la inclusione elettronica, l'amministrazione in rete, la qualità della vita tramite la creazione di trasporti intelligenti, delle biblioteche digitali. Sulla nuova strategia è stato fatto il punto della situazione a piu' riprese: con le comunicazioni COM(2007) 146 def. e COM(2008)199 def.
Dalla Comunicazione della Commissione *"Relazione sulla competitività digitale in Europa: principali risultati della strategia i2010 nel periodo 2005-2009"* (COM(2009) 390 def.) si rileva che sono stati

raggiunti i seguenti risultati:

- il numero dei cittadini europei in linea è notevolmente aumentato, in modo particolare quello delle categorie svantaggiate;
- l'Europa è diventata il leader mondiale dell'internet a banda larga;
- la connettività a banda larga è aumentata;
- L'Europa è al primo posto nella telefonia mobile;
- La fornitura e l'uso dei servizi on line sono notevolmente aumentati;
- Progressi sono stati fatti nel settore delle TIC associate alla micro e alla nano elettronica, alla sanità e alla sicurezza stradale;
- Le politiche TIC fanno sempre di piu' parte della politica generale
- Si registra sempre un notevole ritardo nella ricerca esviluppo tecnologico nelle TIC rispetto a Stati Uniti, Giappone, Corea del Sud.

Nel quadro di questa nuova strategia si colloca il progetto *"Le biblioteche digitali"* (Comunicazione COM (2005) 465 def. del 30.9.2005). Questa iniziativa intende rendere piu' agevole e piu' interessante l'uso delle risorse di informazione europee in linea, valorizzando il vasto patrimonio europeo e combinando i contesti multiculturali e plurilingue con i progresso tecnologici e i nuovi modelli commerciali (pag. 3). Per mettere in comune questo patrimonio ci sono da affrontare diverse difficoltà di tipo finanziario, organizzativo, tecnico, giuridico. Ci sono problemi relativi alla conservazione del patrimonio digitale.
Sulla banda larga si rinvia alla Comunicazione "*Colmare il divario nella banda larga"* (COM(2006) 129 def. del 20.3.2006).
Nell'ambito dell'iniziativa "i2010" viene varato il piano "Invecchiare bene nella società dell'informazione. Piano d'azione su tecnologie dell'informazione e della comunicazione e invecchiamento" (Comunicazione COM(2007) 332 def. del 14.6.2007): l'invecchiamento della popolazione europea rappresenta una sfida per il mercato europeo dell'occupazione, dei sistemi dei servizi e dell'assistenza sanitaria, ma anche una opportunità economica e sociale. Dalle tecnologie dell'informazione e della comunicazione (TIC) scaturiranno infatti prodotti e servizi nuovi, piu' accessibili e atti a rispondere alle esigenze degli anziani.

3.11. La sanità elettronica

Il piano d'azione "Sanità elettronica" si inserisce nel "piano di azione eEurope". L'azione proposta si articolava su tre linee di intervento:

- Soluzioni di problemi comuni a tutti gli Stati Membri dell'UE e creazione di un quadro adeguato a sostegno della sanità elettronica;
- Attuazione di azioni pilota volte ad accelerare l'avvio dell'assistenza sanitaria online;
- Diffusione delle migliori prassi e valutazione dei progressi compiuti;
- Soluzione di problemi comuni.

La Comunicazione "Sanità elettronica – migliorare l'assistenza sanitaria dei cittadini europei: piano di azione per uno spazio europeo della sanità elettronica" (COM (2004) 356 def.) in dettaglio riporta gli obiettivi specifici:

- Creare un ruolo guida delle autorità competenti per la sanità;

- Interoperabilità dei sistemi di informazione sanitaria;
- Mobilità dei pazienti e degli operatori sanitari;
- Migliorare le infrastrutture e le tecnologie;
- Certificazione di conformità dei sistemi sanitari online;
- Stimolare gli investimenti;
- Affrontare una serie di aspetti giuridici e normativi in materia di informazione ai pazienti, di sicurezza e responsabilità degli operatori sanitari, di risk management, ecc.
- Attuazione di progetti pilota;
- Monitoraggio delle buone prassi.

Sulla telemedicina si rinvia alla comunicazione (COM(2008) 689 def. del 4.11.2008) *"Sulla telemedicina a beneficio dei pazienti, dei sistemi sanitari e della società"*.

3.12. Contenuti creativi online

"La disponibilità e l'impiego della banda larga e le maggiori possibilità di accedere ai contenuti e ai servizi creativi ovunque e in qualsiasi momento offrono delle nuove opportunità stimolanti. Per i consumatori questo si traduce in nuovi modi per accedere, se non addirittura per condizionare, i contenuti creativi presenti nelle reti mondiali, come internet, sia da casa che utilizzando dispositivi mobili. Per le imprese significa poter offrire servizi e contenuti nuovi e sviluppare nuovi mercati. Con lo sviluppo di dispositivi, reti e servizi nuovi, queste opportunità devono essere affrontate da operatori di contenuti e di reti, titolari di diritti, consumatori, autorità pubbliche e organi di regolamentazione indipendenti. Le soluzioni piu' appropriate si tradurranno in crescita, occupazione e innovazione in Europa" (pag. 2 della Comunicazione COM(2007) 836 def. del 3.1.2008). Le proposte riportate nella comunicazione:

- Garantire che i contenuti europei contribuiscano nella misura del possibile alla competitività europea e favoriscano la disponibilità e la diffusione dell'ampia diversità della creazione di contenuti europei e del patrimonio linguistico e culturale dell'Europa;
- Aggiornare o chiarire le eventuali disposizioni giuridiche che ostacolano inutilmente la diffusione online dei contenuti creativi online nell'UE, riconoscendo nel contempo l'importanza dei diritti d'autore per la creazione;
- Incoraggiare il ruolo attivo degli utilizzatori nella selezione, diffusione e creazione di contenuti.

Alcuni problemi da risolvere:

- Disponibilità di contenuti creativi;
- Concessione di licenze multi territoriali per i contenuti creativi;
- Interoperabilità e trasparenza dei sistemi di gestione digitale dei diritti (DRM);
- Offerte lecite e pirateria.

3.13. Verso una società dell'informazione accessibile

"La Commissione ritiene ora urgente definire un approccio piu' omogeneo, comune ed efficace alla e-accessibilità, particolare all'accessibilità al web, per accelerare l'avvento di una società dell'informazione accessibile, come annunciato dalla Agenda sociale rinnovata". (pag. 3 della comunicazione COM(2008)804 del 1.12.2008). Nella Comunicazione sono proposte le seguenti azioni:

a) Rafforzare le priorità programmatiche, il coordinamento e la cooperazione tra soggetti interessati;
b) Controllo dei progressi e rafforzamento delle buone pratiche;
c) Sostenere l'innovazione e l'applicazione;
d) Facilitare le attività di normalizzazione;
e) Utilizzare la normativa vigente e prospettarne una nuova.

Sulla accessibilità al web le azioni proposte:

a) Facilitare la rapida adozione ed attuazione di orientamenti internazionali in Europa;
b) Promuovere l'accessibilità del web e migliorarne la comprensione.

3.14. Le tecnologie dell'informazione e della comunicazione per le zone rurali

Per migliorare l'accesso alle tecnologie dell'informazione e della comunicazione nelle zone rurali la Comunicazione COM(2009)103 def. del 3.3.2009 ha proposto alcuni interventi:

- Incentivazione della domanda:contenuti, servizi, applicazioni;
- Intervenire sul divario tra uso delle TIC tra aree urbane e aree rurali;
- Utilizzazione ed ampliamento della infrastruttura della banda larga.

Gli attori penalizzati sono: imprese agricole; piccole e medie imprese e micro-imprese; giovani; donne; anziani e gruppi svantaggiati.

3.15. Le tecnologie dell'informazione e della comunicazione (TIC) per l'efficienza energetica

Il potenziale delle TIC per migliorare l'efficienza energetica è ampiamente riconosciuto ma è necessario definire ed attuare una politica per stimolare l'uso delle TIC nel settore (Comunicazione COM(2009)111 del 12.3.2009: "*Sull'uso delle tecnologie dell'informazione e della comunicazione per agevolare la transizione verso un'economia efficiente sotto il profilo energetico e a basse emissioni di carbonio*").

Le TIC possono consentire incrementi di efficienza energetica; possono fornire la base quantitativa per elaborare, attuare, e valutare strategie di efficienza energetica. In particolare, i

piani di azione dovrebbero permettere di ridurre l'impronta energetica e carbonica delle TIC; di razionalizzare l'uso dell'energia nei trasporti tramite la logistica; incoraggiare un cambiamento di comportamento duraturo dei consumatori, delle imprese e delle comunità nell'uso finale dell'energia.

3.16. Le tecnologie emergenti e future (TEF) in Europa

La ricerca sulle tecnologie emergenti e future (TEF) è fondamentale per rafforzare l'eccellenza e supportare la innovazione. Il Piano TEF viene considerato come "apripista" per le tecnologie dell'informazione "radicalmente nuove" (così a pag. 3 della Comunicazione COM(2009)184 def. del 20.4.2009: "*Nuovi orizzonti delle tecnologie dell'informazione e della comunicazione – una strategia di ricerca sulle tecnologie emergenti e future in Europa"*).
La ricerca nelle TEF è stata lanciata nel 1989 ed il piano europeo di ricerca TEF è unico nel suo modo di combinare tra loro le caratteristiche seguenti:

- Fondamentale, in quanto getta fondamenta nuove per le TIC future;
- Trasformativa, perché ispirata da idee che possono cambiare radicalmente la ricerca;
- Ad alto rischio, ma controbilanciate da ricadute positive;
- Mirata, perché intende influenzare i programmi futuri della ricerca sulle TIC;
- Multidisciplinare, perché si base su diverse discipline;
- Collaborativa, perché riunisce le migliori energie per collaborare su progetti avanzati a livello europeo e mondiale.

Linee d'azione proposte:

- Rafforzare la ricerca sulle TEF nel campo tematico delle TIC (aumento del 20% all'anno, dal 2011 al 2013, del bilancio del 7° Progetto Quadro a favore delle TEF);
- Progetti sui biocomputer;
- Programmazione e iniziative congiunte sulle TEF nell'ambito dello Spazio europeo della ricerca (SER);
- Rafforzare il coinvolgimento dei giovani ricercatori nella ricerca TEF;
- Agevolare lo sfruttamento piu' rapido delle conoscenze scientifiche e accelerare l'innovazione;
- Agevolare la collaborazione con i leader mondiali della ricerca e attirare i talenti di fama mondiale in Europa.

3.17. Competenze informatiche per il XXI secolo

"L'innovazione e l'adozione delle tecnologie dell'informazione e della comunicazione (TIC) sono due aspetti importanti della strategia di Lisbona rinnovata per la crescita e l'occupazione. Il contributo delle TIC all'economia europea è essenziale per l'aumento della produttività e lo sviluppo di prodotti e servizi ad alta intensità di conoscenze. E' importante affrontare

le questioni connesse alle competenze nel campo delle TIC (competenze informatiche o *eSkills*) per soddisfare la crescente domanda di specialisti e utenti di TIC Altamente qualificati, rispondere alle esigenze in rapida evoluzione dell'industria e garantire l'alfabetizzazione informatica di tutti i cittadini in un contesto di apprendimento permanente che richiede la mobilitazione di tutti i soggetti interessati" (pag. 3 della Comunicazione COM(2007) 496 def. del 7.9.2007: *"Competenze informatiche (eSkills) per il XXI secolo: promozione della competitività, della crescita e dell'occupazione"*. Secondo la Comunicazione le competenze strategiche non vengono ancora viste come una sfida strategica a lungo termine. Vi quindi una carenza di impostazione comune a livello della UE e vi è la prevalenza di un approccio frammentario. Si rileva il calo dell'offerta di specialisti delle TIC altamente qualificati. Nella realtà la Comunicazione fa notare che esiste una istruzione formale ed una istruzione in azienda intese come "universi paralleli". L'analfabetismo informatico è ancora consistente. Le azioni individuate dalla Comunicazione mirano quindi ad affrontare globalmente il problema, anche con il supporto dell'eLearning.

3.18. Una strategia per una crescita intelligente, sostenibile e inclusiva

"Il 2010 deve segnare un nuovo inizio. Voglio che l'Europa esca rafforzata dalla crisi economica e finanziaria.[...] Gli ultimi due anni hanno lasciato dietro di sé milioni di disoccupati.Hanno provocato un indebitamento che durerà molti anni.[...] La nostra priorità a breve termine è superare con successo la crisi. Sarà ancora dura per qualche tempo, ma ce la faremo. [...] E' questo obiettivo della strategia Europa 2020: piu' posti di lavoro e una vita migliore. La Commissione propone per il 2020 cinque obiettivi misurabili dell'UE..."(così si esprime il presidente Josè Manuel Barroso a pag. 2 e 3 della Comunicazione della Commissione "Europa 2020. Una strategia per una crescita intelligente, sostenibile e inclusiva" (COM(2010)2020 def. del 3.3.2010).
Tra gli obiettivi definiti nella "crescita intelligente" vi è quello della "Società digitale" oltre agli obiettivi di "innovazione" e "Istruzione". Nell'obiettivo "società digitale" si prevede la costituzione di una agenda europea del digitale.

3.19. Un'agenda digitale europea

L'Agenda digitale europea è una delle sette iniziative faro della strategia "Europa 2020". L' Agenda propone di sfruttare al meglio il potenziale delle tecnologie dell'informazione e della comunicazione (TIC) per favorire l'innovazione, la crescita economica e il progresso (Comunicazione COM(2010)245 def. del 19 maggio 2010*: "Un'agenda digitale europea"*). L'obiettivo generale è quello di sviluppare un mercato unico digitale per condurre l'Europa verso una crescita intelligente, sostenibile e inclusiva.
Gli ostacoli per questa agenda:

- La frammentazione dei mercati digitali;
- La mancanza di interoperabilità;
- L'aumento della criminalità informatica e il rischio di un calo della fiducia nelle reti;
- La mancanza di investimenti nelle reti;
- L'impegno insufficiente nella ricerca e nell'innovazione;
- La mancanza di alfabetizzazione digitale e di competenze informatiche;
- Le opportunità mancate nella risposta ai problemi della società.

La azioni da intraprendere previste dall'Agenda digitale:

- Realizzare il mercato digitale unico (aprire l'accesso ai contenuti on line legali; agevolare le fatturazioni e i pagamenti elettronici; mancanza di fiducia degli utenti; i servizi di telecomunicazioni devono essere unificati);
- Aumentare l'interoperabilità e gli standard (interoperabilità di dispositivi, applicazioni , banche dati, servizi e reti);
- Consolidare la fiducia e la sicurezza on line (contrasto della criminalità informatica e della pornografia infantile on line; applicare la legge sulla riservatezza e sul trattamento dei dati personali);
- Promuovere un accesso ad internet veloce e superveloce per tutti;
- Investire nella ricerca e nell'innovazione;
- Migliorare l'alfabetizzazione, le competenze e l'inclusione nel mondo digitale;
- Vantaggi per la società grazie a un utilizzo intelligente della tecnologia.

4. La normativa sulla Società dell'informazione

L'Unione Europea ha definito una linea di politica comunitaria in materia di Società dell'informazione ed ha dato vita ad un diritto comunitario della società dell'informazione tramite l'adozione di direttive che hanno disciplinato il settore nei diversi aspetti.
Di seguito si elencano le principali direttive con l'intento di completare il quadro della politica e in questa sede non si procede ad una analisi specifica degli aspetti giuridici e normativi:
88/301/CE del 16 maggio 1988, della Commissione delle CE, relativa alla concorrenza sui mercati dei terminali di telecomunicazioni (G.U. CE 63 del 18 agosto 1988)
90/387/CEE del Consiglio relativa all'istituzione del mercato interno per i servizi delle telecomunicazioni e la realizzazione della fornitura di una rete aperta di telecomunicazioni (Network Provision – ONP) (G.U. CEE L del 24 luglio 1990)
90/388/CEE della Commissione CEE relativa alla concorrenza nei mercati dei servizi di telecomunicazioni (G.U. CEE L 192 del 24 luglio 1990)
91/250/CEE del Consiglio delle Comunità europee, del 14 maggio 1991, relativa alla tutela giuridica dei programmi per elaboratore (G.U. CEE L 122 del 17 maggio 1991)
95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (G.U. CE L 281 del 23 novembre 1995)
96/9/CEE del Parlamento europeo e del Consiglio, dell'11 marzo 1996, relativa alla tutela giuridica delle banche dati (G.U. CE L 77 del 27 marzo 1996)

97/7/CE del Parlamento europeo e del Consiglio del 20 maggio 1997 riguardante la protezione dei consumatori in materia di contratti a distanza (G.U. CE L 144 del 4 giugno 1997)
97/13/CE del Parlamento europeo e del Consiglio, del 10 aprile 1997, relativa alla disciplina comune in materia di autorizzazioni generali e di licenze nel settore dei servizi di telecomunicazioni (G.U. CE L 117 del 7 maggio 1997)
97/51/CE del Parlamento europeo e del Consiglio che modifica le direttive del Consiglio 90/38/CEE e 92/44/CEE relative al contesto concorrenziale delle telecomunicazioni (G.U. CE L 295 del 29 ottobre 1997)
97/66/CE: trattamento dei dati personali e tutela della vita privata nel settore delle telecomunicazioni (G.U. CE L 24 del 30 gennaio 1998)
1999/93/CE del Parlamento europeo e del Consiglio, del 13 dicembre 1999, relativa ad un quadro comunitario per le firme elettroniche (G.U. CE L 13 del 19 gennaio 2000)
2000/31/CE del Parlamento europeo e del Consiglio, dell'8 giugno 2000, relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno ("Direttiva sul commercio elettronico") (G.U. CE L 178 del 17 luglio 2000)
2001/29/CE del Parlamento europeo e del Consiglio, del 22 maggio 2001, sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione (G.U. CE L 167 del 22 giugno 2001)
2002/19/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002, relativa all'accesso alle reti di comunicazione elettronica e alle risorse correlate, e all'interconnessione delle medesime (direttiva accesso) (G.U. CE L 108 del 24 aprile 2002)
2002/20/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002, relativa alle autorizzazioni per le reti e i servizi di comunicazioni elettronica (direttiva autorizzazioni) (G.U. CE L 108 del 24 aprile 2002)
2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002, che istituisce un quadro normativo comune per le reti ed i servizi di comunicazione elettronica (direttiva quadro) (G.U. CE L 108 del 24 aprile 2002)
2002/22/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002, relativa al servizio universale e ai diritti degli utenti in materia di reti e servizi di comunicazione elettronica (direttiva servizio universale) (G.U. CE L 108 del 24 aprile 2002)
2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche) (G.U. CE L 201 del 31 luglio 2002)
2002/65/CE del Parlamento europeo e del Consiglio, del 23 settembre 2002, concernente alla commercializzazione a distanza di servizi finanziari ai consumatori e che modifica la direttiva 90/619/CEE del Consiglio e le direttive 97/7/CE e 98/27/CE (G.U.CE L 271 del 23 settembre 2002)
2002/77/CE della Commissione del 16 settembre 2002 relativa alla concorrenza nei mercati delle reti e dei servizi di comunicazione elettronica (G.U. CE L 249 del 17 settembre 2002)
2003/98/CE del Parlamento europeo e del Consiglio del 17 novembre 2003 relativa al riutilizzo dell'informazione del settore pubblico.

5. Considerazioni finali

Facciano un breve bilancio di 20 anni di politica e normativa comunitaria per la Società dell'Informazione:

- Nel 1990 si avvia un processo importante per la liberalizzazione dei mercati e dei servizi di telecomunicazioni;
- Nel 1994 la Commissione Bangemann pone le basi di una politica comunitaria sulla società dell'informazione;
- Nel 2002 si puo' registrare una evoluzione profonda nella politica delle telecomunicazioni: si abbandona l'approccio al settore strettamente legato alle tecnologie e si sposta l'attenzione sulle "comunicazioni elettroniche" e quindi sulle tecnologie per supportare le stesse comunicazioni ma con particolare attenzione ai contenuti digitali; si riformulano le regole quadro generali del settore, le regole in particolare di accesso, di autorizzazione, di servizio universale;
- Particolare attenzione è dedicata alle tematiche e alle problematiche in materia di accessibilità, di tutela dei dati personali, di occupazione, di e-economia, di formazione in rete, di sanità elettronica, ai diritti d'autore e alla tutela del software e delle banche dati, al commercio elettronico;
- Tutta la politica risente di un approccio verticale e quindi senza un approccio globale che non ha permesso di creare un mercato interno delle comunicazioni elettroniche;
- Necessità della politica comunitaria di cambiare rotta se non si vuole perdere la scommessa dei progetti eEurope e di altri progetti di ricerca e sviluppo del settore: l'Agenda digitale è il simbolo di questo cambiamento;
- Come procedere: sburocratizzando i piani; piu' interventi di controllo politico sulle azioni da avviare e sui progetti avviati; definire i piani dell'Agenda digitale con un approccio finalizzato allo sviluppo di mercati piu' sensibilizzati ai contenuti digitali e ai servizi informativi a valore aggiunto; definire skills nuovi per attività nuove; nuove politiche del lavoro in relazione a nuovi mercati e ai nuovi profili professionali e lavorativi; spingere le università a sostenere queste politiche per formare nuovi skills per nuovi mercati.
- L'Agenda digitale ha indicato con chiarezza tutti i vincoli esistenti per questa nuova fase della politica per la Società dell'informazione.

Rivista elettronica di Diritto, Economia, Management

N. 1 - 2010 · pp. 30-67

Profili e problemi della disciplina sul Commercio Elettronico a dieci anni dalla direttiva 2000/31

Leonardo Bugiolacchi

Abstract: Nell'anno 2000 l'elaborazione, da parte della Commissione europea, di una direttiva che fornisse un quadro giuridico di riferimento per il nuovo mercato elettronico rappresentò un importante laboratorio per la costruzione del rapporto tra diritto e tecnologie dell'informazione e della comunicazione, mediando tra conservazione dell'esistente e introduzione di nuove regole. Oggi, a distanza di oltre dieci anni, è possibile affermare che tale scelta fu corretta? Il bilancio è in linea di massima positivo, anche se è impossibile negare che, mentre l'ambito della contrattazione telematica ha raggiunto un livello elevato di efficienza, il regime di responsabilità degli internet provider disegnato dalla direttiva, caratterizzato da una eccessiva genericità iniziale, non si è dimostrato in grado di governare l'evoluzione dei servizi offerti in rete, generando disarmonie tra le discipline di recepimento degli stati membri e incertezza interpretativo nel nostro diritto interno. Il presente scritto si propone quindi di tracciare un primo, seppur parziale bilancio, su alcuni profili rilevanti della disciplina italiana sul commercio elettronico.

1. Premessa

Sono trascorsi ormai oltre dieci anni dalla pubblicazione, sull'allora Gazzetta Ufficiale delle Comunità europee (era il 17 luglio 2000), della direttiva 2000/31 relativa a "taluni aspetti giuridici dei servizi della società dell'informazione nel mercato interno, con particolare riferimento al commercio elettronico, ed oltre sette dall'entrata in vigore del testo normativo con il quale il legislatore interno italiano l'ha recepita (d.lgs. n. 70 del 2003).

Con quell'intervento il legislatore sovranazionale prese atto dell'ormai avvenuta transizione dello sviluppo della rete verso la sua fase di diffusione e, consapevole delle grandi potenzialità offerte dall'e-commercio per lo sviluppo del mercato interno e per la creazione di occupazione, soprattutto nel settore delle piccole e medie imprese, intese apprestare un

Articolo pervenuto il 4 ottobre 2010, approvato il 22 novembre 2010

quadro giuridico di riferimento armonizzato per il nuovo fenomeno.

Non vi è dubbio che la nascita e lo sviluppo del "commercio elettronico" abbiano rappresentato una delle conseguenze più evidenti dell'odierna società globalizzata, quella che è ormai conosciuta come "società dell'informazione", nella quale le nuove tecnologie informative e comunicative consentono di affiancare ai mercati tradizionali (fisici) nuovi ambienti di scambio di beni e servizi, oltre che di condivisione della conoscenza[1].

Al mercato inteso in senso fisico si sostituisce un luogo virtuale, un marketplace elettronico, al quale si accede per mezzo delle nuove tecnologie, ed il commercio elettronico diviene così uno dei fenomeni caratterizzanti l'odierna società dell'accesso, come felicemente definita qualche anno fa dallo studioso americano Jeremy Rifkin.

L'accesso all'ambiente interconnesso diviene da un lato precondizione della fruizione di beni e servizi, dall'altro, molto spesso, modalità stessa di fruizione dei servizi richiesti, in un quadro in cui mercati cedono il posto alle reti, i venditori e i compratori divengono rispettivamente fornitori e utenti, ed il godimento di qualunque bene, anche quello della conoscenza, derivante dall'accessibilità ad una mole sconfinata di informazioni, si può ottenere attraverso l'accesso[2].

In questo nuovo mercato reticolare, basato sull'interconnessione di venditori e acquirenti, ora divenuti prestatori e destinatari di servizi, l'accesso al luogo di scambio è reso molto più agevole per tutti i protagonisti, dato che gli imprenditori medi e piccoli possono infatti raggiungere un numero potenzialmente molto elevato di consumatori e utenti, mentre questi ultimi vedono aumentare a dismisura l'accessibilità a prodotti e servizi, peraltro a prezzi convenienti, in quanto condizionati dall'elevata concorrenza e dalla riduzione dei costi di distribuzione da parte dei fornitori[3].

In questo arco temporale decennale che ormai ci separa dalla pubblicazione della "direttiva e-commerce" l'ambiente nel quale il commercio elettronico e, più in generale, i servizi della società dell'informazione si svolgono sono stati interessati da notevoli cambiamenti, dovuti, ancora una volta, alla evoluzione degli strumenti tecnologici.

Se infatti all'epoca della gestazione della direttiva il marketplace elettronico era strutturato

---

[1] L'espressione società dell'informazione designa l'attuale fase di sviluppo della parte più avanzata del mondo e si riferisce all'importanza sempre crescente che possiedono in essa le tecnologie dell'informazione e della comunicazione, sia grazie all'avvento della telematica che al processo di liberalizzazione nel settore telecomunicativo. Tale espressione si rinviene per la prima volta nel Rapporto Delors del 1993, nel quale la società dell'informazione è considerata una dimensione nuova ed essenziale per il rilancio dell'economia europea; viene poi ripresa nel 1994 nel cosiddetto rapporto Bangemann, con il quale sono state poste le basi per la definizione di un quadro normativo per la società dell'informazione.

[2] Rifkin, L'era dell'accesso, Milano, 2000, 9.

[3] E' evidente che il commercio elettronico non è che una delle attività che possono essere svolte mediante le tecnologie dell'informazione e della comunicazione, le quali, in generale, rappresentano uno strumento di accrescimento delle conoscenze, anche attraverso il reperimento di una grande mole di informazioni, nonché un mezzo di esercizio della libertà di manifestazione la cui facile accessibilità non è paragonabile a quella dei tradizionali mezzi di diffusione del pensiero. Un'interessante analisi di internet quale forma di comunicazione in grado di realizzare la libertà costituzionale di manifestazione del pensiero è contenuta nella nota sentenza della Corte Federale del Distretto orientale della Pennsylvania dell'11 giugno 1996 (in Dir. informazione e informatica, 1996, 604).

fondamentalmente come la somma di tanti negozi on line, attraverso i quali il prestatore di servizi offriva i suoi beni ad una platea indistinta di destinatari, negli anni successivi a tali realtà se ne sono aggiunte altre, organizzate come grandi contenitori di offerte di beni o servizi, i cc.dd. portali, nei quali la "merce" offerta poteva essere di proprietà del titolare del portale, come pure, sempre più spesso, di proprietà degli iscritti al portale, il cui titolare svolgeva un ruolo di semplice intermediazione o, addirittura, di puro fornitore di uno spazio web ove si svolgeva l'incontro tra offerta e domanda.

Tale diverso modello ha prodotto problematiche giuridiche nuove, connesse soprattutto alla questione della eventuale responsabile del fornitore dello spazio per eventuali violazioni commesse dagli utenti (dalla vendita di beni rispetto ai quali il venditore non era titolare di diritti di utilizzazione economica, alla mancanza nella cosa offerta in vendita delle qualità promesse, alla non conformità del bene al contratto, etc., come si è già verificato ipotizzando, in tali fattispecie, il coinvolgimento di e-bay[4]).

Contestualmente, la rete ha cominciato sempre più a strutturarsi come strumento di condivisione di contenuti immessi dagli utenti della rete, attraverso l'uploading degli stessi su quelle grandi piattaforme digitali che per tale motivo vengono denominate ugc (user generated content).

La diffusione di tali sistemi di sharing, tra i quali ben possono farsi rientrare i noti Youtube, il servizio Google Video, come pure i social networks quali facebook, twitter, etc., i quali non sono scevri da una componente commerciale (insita nella raccolta pubblicitaria e nella pubblicità, non ricercata ma "subita" che tali spazi generano, ha creato un rapporto del tutto nuovo tra l'intermediario che assicura la memorizzazione permanente e la mole sterminata dei contenuti caricati: ne risulta una modifica del ruolo del provider di hosting, il quale, se già non poteva essere in grado di effettuare (né tecnicamente ma neppure giuridicamente) un controllo sulla liceità degli uploading nella fase in cui, oltre 10 anni fa, egli si limitava ad ospitare, su una porzione del proprio server, le informazioni inserite dall'unico soggetto abilitato ad operare quale content provider del proprio sito web, attualmente è assolutamente impossibile: è assolutamente inesigibile che il provider possa sorvegliare i milioni di contenuti presenti su queste mastodontiche piattaforme. Queste ultime, peraltro, ed in ciò risiede un'altra novità, sono organizzate mediante sofisticati meccanicismi di categorizzazione/indicizzazione e ricerca che, agevolando il reperimento dei contenuti, aumentano anche la possibilità di accedere al materiale ricercato, che ottiene in tal modo maggior visibilità rispetto a quella che avrebbe posseduto sul solo sito ove era stato, eventualmente, caricato all'origine, rendendo in tal modo maggiormente percepibile la lesione e/o la violazione da parte degli stessi danneggiati.

Se al momento, quindi, della gestazione della direttiva, si aveva in mente un host provider che garantiva il mantenimento in rete di una molteplicità di siti web, tendenzialmente riempiti di informazioni dal content provider gestore del sito, assistiamo ora ad una attività

[4] In particolare, sulla tematica del possibile coinvolgimento di E-bay negli illeciti commessi dai suoi utenti, si veda in dottrina BERLIRI e LA GUMINA, La (non) responsabilità di Ebay per gli illeciti commessi dai propri utenti, in Dir. internet, 2007, 342

di hosting operata da un numero abbastanza ristretto di provider, i quali si trovano però ad ospitare una quantità enorme, solo qualche anno inimmaginabile, di contenuti forniti da un numero indiscriminato di utenti.

Non solo. La libera attività di uploading su tali piattaforme fa sì che esse raccolgano materiali molto spesso protetti dalle regole sulla protezione delle opere dell'ingegno o della proprietà industriale, con conseguente lesione, su vastissima scala, dei diritti di utilizzazione economica spettanti ai titolari (rappresentate soprattutto da grandi imprese produttrici di opere protette, televisive, musicali, cinematografiche, etc.).

Una tale situazione, evidentemente diversa rispetto a quella avuta presente dal legislatore europeo in sede di elaborazione della direttiva, richiederà probabilmente una cooperazione tra hosting provider e titolari dei diritti, finalizzata ad individuare i contenuti illegalmente caricati, fermo restando che l'eventuale iniziativa di disabilitazione dell'accesso agli stessi, da parte dei provider, rischia comunque di contrastare con i presupposti legali dell'obbligo di rimozione, che il legislatore italiano del recepimento ha inequivocabilmente collegato alla comunicazione al provider, da parte delle autorità competenti, dell'illiceità dell'informazione.

In questo quadro, il presente lavoro si prefigge di passare in rassegna lo stato dell'arte rispetto a tre principali profili: qualificazione giuridica e fondamento normativo del ruolo dei vari prestatori di servizi della società dell'informazione; procedimento di conclusione del contratto concluso telematicamente; responsabilità civile dell'internet provider, con particolare riferimento al provider di hosting ed alle condizioni della sua responsabilità rispetto ai contenuti caricati dagli utenti sulle piattaforme digitali.

All'esito verrà tentato un bilancio sulla idoneità dell'intervento legislativo europeo e, soprattutto, della disciplina di recepimento, a regolare un fenomeno complesso, caratterizzato dallo svolgimento di attività giuridicamente rilevanti di stampo tradizionale (contratti, illeciti, etc.), realizzate però con modalità nuove. Si ricorderà infatti come, nel quadro del dibattito che coinvolse la civilistica italiana e straniera circa la necessità o, quanto meno, opportunità di introdurre regole ad hoc che disciplinassero le attività svolte con le nuove tecnologie dell'informazione e della comunicazione, la scelta finale, tra l'introduzione di un nuovo diritto, sorta di ius singulare ed il mantenimento integrale delle regole preesistenti, fu per una opzione intermedia: si ritenne cioè che le nuove tecnologie, pur non incidendo sulle categorie e regole tradizionali richiedessero, comunque, nuove regole, necessarie per rendere compatibili quelle esistenti con le nuove modalità tecnologiche di svolgimento dell'attività giuridica[5].

Tutto questo tenendo presente che la valutazione altamente positiva che gli organi co-

[5] Tale dibattito ha dato luogo anche a numerosi convegni, tra i quali si ricorda quello svoltosi a Salerno nel 2001, i cui atti sono stati oggetto di interessante pubblicazione (SICA e STANZIONE, a cura di, Commercio elettronico e categorie civilistiche, Milano, 2002.
In argomento, si veda ALPA, Cyberlaw. Problemi giuridici connessi allo sviluppo di internet, in Nuova giur. Civ. comm., 1998, II, 385. Sia consentito anche il rinvio a BUGIOLACCHI e VIOLA, Il rapporto tra il diritto e le nuove tecnologie dell'informazione e della comunicazione. Il diritto dell'informatica, in PALAZZOLO (a cura di), L'informatica giuridica oggi, Atti del convegno ANDIG, Roma 1° dicembre 2005, Napoli, 2007, 106.

munitari fecero del commercio elettronico, nell'ormai lontano 1998, allorchè ebbe inizio l'iter che condusse all'emanazione della direttiva 2000/31 fu tutt'altro che illusoria o caratterizzata da eccessivo entusiasmo, se è vero che ancora la recentissima Risoluzione del Parlamento europeo del 21 settembre 2010 sul completamento del mercato interno per il commercio elettronico non ha mancato di evidenziare, sotto molteplici profili, il rilevantissimo ruolo dell'e-commerce nel rilancio del mercato interno unico, tanto da considerarlo un "mercato chiave del XXI secolo, potenzialmente in grado di rimodellare il mercato interno europeo, di contribuire all'economia della conoscenza, di generare valore e opportunità per i consumatori e le imprese in questo periodo di difficoltà finanziarie"[6] e, se è vero, come è vero, che l'e-commerce sta conoscendo uno sviluppo esponenziale, tanto da rappresentare rispetto a talune categorie merceologiche e di servizi, una quota rilevante dell'intero mercato.

2. Servizi della società dell'informazione (ssi), servizi di comunicazione elettronica e disciplina degli intermediari.

È noto come grazie alle tecnologie trasmissive standardizzate (i protocolli), oltre che attraverso l'uso di un modem, collegato ad un apparecchio telefonico o ad altro terminale idoneo (mobile phone) è possibile fare ingresso nella rete, la quale costituisce l'ambiente del commercio elettronico.
Affinché però l'utente finale (intendendo con ciò il singolo che intende accedere, a partire dal proprio terminale, alla rete per fruire della massa informativa disponibile oppure agire, ove lo voglia, quale venditore o acquirente di beni e/o servizi on-line) possa ottenere la connessione è necessaria l'attività di altri soggetti, fornitori di servizi informatici.

Gli utenti accedono infatti alla rete attraverso una molteplicità di mezzi, ma tendenzialmente le modalità di accesso sono due.

In primo luogo si può utilizzare un elaboratore o un terminale di elaboratore che è direttamente e permanentemente collegato ad una rete di elaboratori che è a sua volta collegata direttamente o indirettamente a Internet.

In secondo luogo (ed è questa la modalità di connessione degli utenti privati) si può utilizzare un computer dotato di modem per collegarsi attraverso la linea telefonica ad un elaboratore o ad una rete più potente che sono direttamente o indirettamente collegati ad Internet.

I soggetti che offrono tale servizio di accesso agli utenti finali sono i cosiddetti provider, i quali molto spesso coincidono con i gestori delle linee telefoniche nazionali o internazionali (ed allora sono denominati provider di "primo livello" – solitamente definiti NSP, Network Service Provider, come ad esempio Telecom) i quali, talvolta, già dispongono delle infrastrutture comunicative necessarie, mentre altre volte sono soggetti che ottengono, dietro corrispettivo

[6] Così, testualmente, il considerando "F" della Risoluzione.

di un canone, la disponibilità da parte dei medesimi gestori delle reti telecomunicative di infrastrutture di trasmissione grazie alle quali stabiliscono collegamenti permanenti con la rete, finalizzati alla fornitura di servizi agli utenti finali (e sono i provider di "secondo livello"). In questo caso è corretto affermare come il provider (di secondo livello) rappresenti l'interfaccia di due rapporti contrattuali: uno con il network provider (il gestore della rete, in virtù di un'autorizzazione statale), dal quale ottiene la connettività, l'altro con l'utente al quale offre i propri servizi, sempre nell'ambito di un rapporto contrattuale.

I provider, i quali offrono anche ulteriori servizi, rispetto ai quali la fornitura dell'accesso è propedeutica (si pensi a quello di utilizzazione della posta elettronica, a quella di predisposizione di un sito web, contraddistinto da apposito nome di dominio, etc.), svolgono la loro attività professionalmente, impegnando a proprio rischio una organizzazione di mezzi non indifferente.

Come è noto, negli ultimi anni l'attività imprenditoriale di tali soggetti, che si è sempre più incentrata sulla messa a disposizione di una mole enorme di contenuti (attività di hosting), forniti dagli stessi utenti in un meccanismo di continuo sharing di informazioni, si svolge senza che venga richiesto un corrispettivo per l'accesso alla piattaforma informativa, rinvenendo tali provider la loro remunerazione nella realizzazione del miglior abbinamento tra le informazioni e i messaggi pubblicitari degli inserzionisti.

In questa ottica, il servizio base di accesso ad internet, il quale viene ormai pacificamente qualificato come contratto di appalto di servizi, grazie alla diffusione di tariffe cc.dd. flat è assurto al ruolo di commodity, in quanto è percepito dagli stessi titolari del servizio di gestione delle piattaforme di contenuti, quale precondizione per l'accesso all'ampia gamma di servizi fruibili nel marketplace elettronico, dai quali il provider ottiene il suo effettivo profitto secondo i nuovi modelli commerciali elaborati in questi ultimi anni[7].

Un aspetto della disciplina dei provider che non è stato oggetto di analisi nella pur vastissima letteratura prodotta nel nostro paese a far data dalla pubblicazione del decreto di recepimento della direttiva 2000/31, è quello relativo alla qualificazione giuridica di tali soggetti.

Si tratta, a ben vedere, di un profilo abbastanza complesso.

Intanto, non vi è dubbio che gli isp che forniscono i servizi mediante i quali la rete è fruibile in tutte le sue potenzialità (access provider, di primo o secondo livello e, ottenuta la connessione, fondamentalmente i provider di hosting) siano qualificabili come "prestatori" (di servizi della società dell'informazione), ai sensi dell'art. 2, primo comma, lett. b) del d.lgs. n. 70 del 2003, in quanto tale disposizione definisce il prestatore "la persona fisica o giuridica che presta un servizio della società dell'informazione".

Non vi è infatti dubbio che il servizio (o i servizi) prestati da tali soggetti rappresentino "servizi della società dell'informazione". Questi ultimi, secondo la definizione di cui all'art. 2, lett. a) del d.lgs. 70/2003, aspramente criticata in dottrina[8] in quanto generica ed in quanto costruita

---

[7] Si pensi, tanto per fare un esempio, al programma ADWords, implementato da Google, il quale gestisce i contenuti caricati dagli utenti sulla piattaforma messa a disposizione dal provider di hosting con finalità di facilitazione e targettizzazione della raccolta pubblicitaria.

[8] Si veda ZENO ZENCOVICH, La nuova disciplina del commercio elettronico alla luce del d.lgs. 70/03: questioni

alquanto cripticamente attraverso un rinvio ad altro testo normativo, vengono individuati sia con riferimento ad ogni attività economica svolta on-line, sia come quei servizi definiti appunto per relationem, mediante il rinvio operato dalla medesime lettera ad una disposizione della legge 317 del 1986[9].

E' bene precisare che la stessa attività di "commercio elettronico", pur mancante di una definizione espressa da parte del decreto 70/2003 rappresenta un "servizio della società dell'informazione", come risulta inequivocabilmente, pur se indirettamente, dal testo dell'art. 1, n. 1 del d.lgs. 70/2003, ove infatti si legge che "il presente decreto è diretto a promuovere la libera circolazione dei servizi della società dell'informazione, fra i quali il commercio elettronico".

A ben vedere, però, prestatore di un servizio della società dell'informazione è anche e soprattutto qualunque soggetto che intenda esercitare quello specifico servizio qualificato come commercio elettronico, al fine di proporre beni e servizi nel mercato elettronico, e che trova la sua "controparte" nel "destinatario del servizio", definito dalla lettera d) del citato art. 2, come il "soggetto che, a scopi professionali o non , utilizza un servizio della società dell'informazione, in particolare per ricercare o rendere accessibili informazioni"[10].

Questo significa che l'importante apparato di obblighi che la direttiva prima ed il decreto di recepimento poi addossano ai prestatori di servizi della società dell'informazione, riguarda sia quelli che potremmo definire "intermediari necessari" del commercio elettronico (in quanto fornitori di servizi propedeutici e necessariamente strumentali all'intrapresa di una attività commerciale on line, dall'accesso alla rete alla fornitura dello spazio web grazie al quale allestire un negozio virtuale) che gli operatori commerciali on line in senso stretto (venditori di beni e/o servizi). In questo senso, direttiva e decreto impongono i medesimi obblighi a questi prestatori, pur nella diversità fattuale delle loro attività.

Questo quadro di indistinta applicabilità a tutti i prestatori di ssi (servizi società dell'informazione) delle disposizioni della normativa di recepimento viene però contraddetto da quella serie di disposizioni (artt. 14-17 d.lgs. n. 70/2003) che compongono il regime speciale di

generali e ambito di applicazione, in TOSI (a cura di), Commercio elettronico e servizi della società dell'informazione, Milano, 2003, 45.

[9] Il rinvio operato dall'art. 2, lett. a), d.lgs. 70/2003 è alla nozione di servizio di cui all'art. 1, comma 1, lett. b) della l. 317/1986, secondo il quale per "servizio della società dell'informazione" deve intendersi: "qualsiasi servizio della società dell'informazione, vale a dire qualsiasi servizio prestato normalmente dietro retribuzione,a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi. Ai fini della presente definizione si intende: per 'servizio a distanza' un servizio fornito senza la presenza simultanea delle parti; per 'servizio per via elettronica' un servizio inviato all'origine e ricevuto a destinazione mediante attrezzature elettroniche di trattamento, compresa la compressione digitale e di memorizzazione di dati e che è interamente trasmesso, inoltrato e ricevuto mediante fili, radio, mezzi ottici od altri mezzi elettromagnetici; per 'servizio a richiesta individuale di un destinatario di servizi' un servizio fornito mediante trasmissione di dati su richiesta individuale.

[10] E' stato correttamente osservato (MANNA, La disciplina del commercio elettronico, Padova, 2005, 11; SCORZA, I l consumatore telematico, in CASSANO (a cura di), Commerci o elettronico e tutela del consumatore, Milano, 2003, 37) come tale figura costituisca un novum nel panorama giuridico, in quanto più ampia di quella di consumatore. La ratio è quella di estendere la protezione riservata al consumatore anche al di là della nozione restrittiva che di tale soggetto è data dalla normativa comunitaria, al fine di attribuire alla controparte del prestatore di servizi una serie di strumenti che gli consentano di riequilibrare il gap informativo sussistente tra i due, come risulta confermato dal fatto che gli obblighi informativi imposti dal d.lgs. 70/2003, proprio in funzione di protezione del contraente debole, vedono come beneficiario il "destinatario del servizio", soggetto la cui nozione è più ampia di quella di consumatore.

responsabilità degli internet provider, la cui applicabilità risulta invece limitata espressamente ai soli fornitori di trasporto dati - mere conduit (art. 14), di memorizzazione temporanea – caching (art. 15) e di memorizzazione tendenzialmente permanente –hosting (art. 16): rispetto a tali attività specifiche, caratterizzate da una situazione di crescente vicinanza alle informazioni trasmesse in rete, è infatti possibile ipotizzare, in presenza delle condotte in queste disposizioni tipizzate, una responsabilità di tali soggetti per gli illeciti commessi dai loro utenti.

Deve però essere tenuto presente che l'attività dei prestatori di ssi – o meglio, come stiamo per vedere, di taluni di essi - non è disciplinata soltanto dai regolamenti contrattuali dai medesimi stipulati con gli utenti o eventualmente (nel caso dei provider di secondo livello) con i gestori delle linee telecomunicative (provider di primo livello), oltre che da quanto previsto dal d.lgs. n. 70 del 2003[11].

Ciò in quanto i prestatori che si pongono quali intermediari necessari della rete (internet service provider, isp in senso stretto) risultano destinatari di ulteriori disposizioni di legge, per il fatto che in talune situazioni l'internet service provider possiede anche una rilevanza pubblicistica, risultante da una serie univoca di indici normativi.

La regolazione amministrativa che ne deriva, sebbene sembri esulare dalla presente indagine, deve essere quanto meno brevemente tratteggiata al fine di comprendere le sovrapposizioni ed evitare errate interpretazioni originate dalle disposizioni definitorie contenute in tale regolazione.

La fornitura di accesso alla rete, come peraltro ogni altra fornitura di servizio telecomunicativo (ora, più esattamente, definito come servizio di comunicazione elettronica) e, nella prospettiva che ci riguarda, ogni attività di trasmissione di segnali (e quindi informazioni) su reti, anche dopo la liberalizzazione comunitaria avvenuta nel settore delle telecomunicazioni, restano attività sottratte al libero dispiegarsi delle dinamiche di mercato e continuano pertanto ad essere destinatarie delle limitazioni e dei controlli che anche il nostro ordinamento è legittimato ad adottare nei confronti dell'iniziativa economica privata a tutela di valori di rango costituzionale[12].

Sebbene la direttiva comunitaria che ha dato inizio al processo di liberalizzazione accennato (direttiva n. 97/13) non menzionasse mai espressamente Internet, la sua applicabilità alla rete è fin da subito risultata indubitabile, avendo il legislatore comunitario univocamente individuato (nel considerando n. 7) tra i servizi telecomunicativi oggetto del provvedimento anche quelli tipicamente veicolabili attraverso Internet, vale a dire l'accesso a basi di dati, i servizi informatici a distanza, la posta elettronica e il trasferimento elettronico di dati per uso commerciale.

D'altronde, dal punto di vista della qualificazione giuridica, la stessa internet, quale luogo

---

[11] Oltre che, per completezza, anche dalle discipline settoriali che il d.lgs. n. 70 del 2003, in più disposizioni, fa salve con apposite "clausole di salvaguardia"; si pensi, ad esempio, al terzo comma dell'art. 1, ed al terzo comma dell'art . 3 del d.lgs. n. 70 del 2003.

[12] Sulla disciplina delle comunicazioni elettroniche, a seguito dell'entrata in vigore del d.lgs. n. 259 del 2003, possono vedersi RANGONE, La disciplina delle comunicazioni elettroniche, in Giornale dir. Amm., 2004, 1173; LIBERTINI, Regolazione e concorrenza nel settore delle comunicazioni elettroniche, ivi, 2005, 195.

virtuale di svolgimento dell'e-commerce, costituisce una "rete di comunicazione elettronica".

Tale qualificazione si rinviene nel Codice delle Comunicazioni elettroniche (d. lgs. 259 del 2003), il quale, all'art. 1, lett. dd), offre appunto la seguente definizione di reti di comunicazione elettronica: "i sistemi di trasmissione e, se del caso, le apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, comprese le reti satellitari, le reti terrestri mobili e fisse, a commutazione di circuito e a commutazione di pacchetto, compresa Internet ...".

E' singolare osservare che, nonostante la sua rilevanza assolutamente centrale, Internet non venga mai menzionata nel d.lgs. 70 del 2003: la sua esistenza e nozione, come anche per la nozione di commercio elettronico, vengono soltanto presupposte[13].

A ben vedere, però, il d.lgs. 70/2003 evoca la rete internet ogni volta che menziona i servizi della società dell'informazione, dato che questi, secondo la già ricordata definizione contenuta nell'art 2, n. 1, consistono appunto nelle attività economiche svolte "on line" (oltre che nei servizi individuati dall' 1, comma 1, lett. b) della l. 317 del 1986, i quali pure, comunque, vengono prestati a distanza e quindi mediante una rete).

E' quindi di tutta evidenza che lo svolgimento "in linea" di tali attività presuppone l'esistenza di una rete, che ad oggi è da individuare in Internet, sebbene nulla impedisca di ritenere che in un futuro anche prossimo possano svilupparsi reti diverse da essa, vale a dire, in sostanza, non necessariamente caratterizzate dalla medesima natura aperta e globalizzata; anche la prestazione di servizi della società dell'informazione su queste reti alternative, in quanto effettuata appunto on line, rientrerebbe nel commercio elettronico[14].

Il citato Codice delle comunicazioni elettroniche, all'art. 25 (intitolato "Autorizzazione generale per le reti e i servizi di comunicazione elettronica"), sancisce che l'attività di fornitura di reti o di servizi di comunicazione elettronica, tra le quali rientra inequivocabilmente, come appena detto, anche l'attività degli ip (internet provider), di cui ci stiamo occupando, è sostanzialmente libera, alle condizioni previste dal decreto medesimo. Ciò significa, in estrema sintesi, che lo svolgimento di tale attività è assoggettato al rilascio di un'autorizzazione generale, che consegue alla presentazione, da parte dell'impresa interessata, al Ministero delle Comunicazioni, di una dichiarazione contenente l'intenzione di iniziare tale attività di fornitura di reti o di servizi di comunicazione elettronica. Il rilascio è subordinato alla verifica da parte del Ministero, della sussistenza dei requisiti richiesti, previsti nel capo II ("Autorizzazioni") del Titolo II ("Reti servizi di comunicazione elettronica ad uso pubblico") del Codice delle Comunicazioni elettroniche[15].

---

[13] Anche la direttiva 2000/31, della quale il d.lgs. 70/2003 costituisce recepimento, non menziona Internet, la quale viene invece presa in considerazione dal considerando n. 2 della direttiva stessa, laddove viene affermato che gli effetti benefici per l'economia e la competitività europee che vengono ricollegati allo sviluppo del commercio elettronico sono subordinati alla condizione che internet sia accessibile a tutti.

[14] A ben vedere, già attualmente stanno nascendo reti che, attraverso una tecnologia analoga a quella di internet, se ne differenziano per la mancanza, di fatto, di accessibilità libera e generalizzata (un esempio sono le reti che si stanno sviluppando in Cina, grazie alla circostanza che questo paese ha creato tre domini con caratteri cinesi, impedendo così agli utenti non cinesi di accedervi – si veda su questo aspetto Il Sole – 24 ore del 22 gennaio 2006, pag. 5).

[15] La necessità di detta autorizzazione risulta confermata, implicitamente, ma al tempo stesso inequivocabilmente,

Ciò detto in via generale, è opportuno precisare che gli internet provider ai quali fa riferimento la disciplina del Codice comunicazioni elettroniche sono soltanto quelli che effettuano servizi di fornitura di reti o di servizi di comunicazione elettronica, vale a dire, ai sensi dell'art. 1, lett., gg), consistenti "esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazione elettronica", quale appunto è Internet.

Tali servizi sono proprio quelli che abbiamo qualificato come propedeutici allo svolgimento del commercio elettronico, in quanto consentono la trasmissione e memorizzazione di segnali (e quindi di informazioni) nel mercato elettronico rappresentato dalla rete.

Laddove invece il prestatore offra servizi differenti da quello, esclusivo o prevalente, di trasmissione di segnali su reti di comunicazione, risulterà escluso dalla disciplina pubblicistica di cui al codice delle comunicazioni elettroniche, come risulta espressamente dalla appena menzionata parte finale della lett. gg) dell'art. 1, ove è previsto che siano esclusi dai servizi di comunicazione elettronica quelli della società dell'informazione di cui al decreto di recepimento della direttiva sul commercio elettronico, ove non consistenti interamente o prevalentemente nella trasmissione di segnali su reti di comunicazione elettronica.

Tale ultima precisazione, che non è stata oggetto di particolare indagine da parte della dottrina, è estremamente importante.

Si è voluto infatti in questo modo, del tutto correttamente, differenziare l'attività dei prestatori di servizi comunicativi di base (accesso, trasporto e, deve ritenersi anche memorizzazione temporanea e permanente in quanto comunque implicanti un preventivo istradamento dei segnali sulle reti), che, in quanto tali, sono assoggettati all'autorizzazione generale di cui all'art. 25 d.lgs. n. 259 del 2003, da quella effettuate dai prestatori di servizi della società dell'informazione, così evitando che si ingenerassero dubbi circa l'eventuale necessità di ottenere la citata autorizzazione anche da parte di coloro che volessero effettuare offerta di beni o servizi on line (vale a dire proprio gli attori del commercio elettronico)[16].

L'aspetto interessante che risulta da questo excursus normativo è che vi sono alcuni soggetti, quali i provider di cui agli artt. 14, 15 e 16 del d.lgs. n. 70 del 2003 che riuniscono in sé sia la

anche dalla recentissima delibera n. 131/06 della Autorità per le Garanzie nelle Comunicazioni (pubblicata sulla G.U. del 27 luglio 2006), la quale, nell'approvare la direttiva in materia di qualità dei servizi di accesso a internet da postazione fissa (vale a dire da parte dell'utente finale, ossia la persona fisica o giuridica che utilizza o chiede di utilizzare un servizio di comunicazione elettronica accessibile al pubblico), che deve essere garantita dalle imprese fornitrici (i provider), definisce queste ultime appunto come i soggetti titolari di autorizzazione, conseguita ai sensi del Codice delle comunicazioni elettroniche, alla fornitura di reti o servizi di comunicazione elettronica accessibili al pubblico.

[16] L'interpretazione proposta pare confermata dal dettato dell'art. 6 d.lgs. 70/2003, di recepimento della direttiva comunitaria in materia di commercio elettronico, il quale, dopo aver affermato, al primo comma, che l'accesso all'attività di prestatore di un servizio della società dell'informazione e il suo esercizio non sono soggetti, in quanto tali, ad autorizzazione preventiva, nel secondo comma, precisa che sono fatte salve le disposizioni sui regimi di autorizzazione (che quindi si applicano), a patto che non riguardino specificamente i servizi della società dell'informazione o i regimi di autorizzazione nel settore dei servizi di telecomunicazioni (che sono appunto quelli che, attualmente, sono oggetto di disciplina da parte del codice com. el.), dalla cui applicazione sarebbero esclusi i servizi della società dell'informazione; in senso analogo anche il II comma dell'art. 4 della direttiva 2000/31, laddove afferma che sono fatti salvi i sistemi di autorizzazione che non riguardano specificatamente ed esclusivamente i servizi della società dell'informazione o i sistemi di cui alla direttiva 97/13 relativa alla disciplina comune in materia di autorizzazioni generali e licenze individuali nel settore dei servizi di telecomunicazioni.

qualifica normativa di prestatori di servizi della società dell'informazione (ai sensi appunto del d.lgs. n. 70 del 2003) che quella di fornitori di servizi di comunicazione elettronica (ai sensi del d.lgs. n. 259 del 2003) [17].

Deve anche ritenersi che gli Internet service providers, proprio in qualità di fornitori di servizi di comunicazione elettronica, siano sottoposti ad un ulteriore controllo di natura amministrativa. Si tratta dell'iscrizione nel Registro degli Operatori di comunicazione, previsto dall'art. 1, comma 6, lett. a), nn. 5 e 6 della legge 31 luglio 1997 n. 249 ed attualmente confermata, nella sua obbligatorietà per chi effettua servizi di comunicazione elettronica, dall'art. 25, comma 4, del codice comunicazioni elettroniche e la cui tenuta è affidata alla già menzionata Autorità di garanzia (registro creato con delibera 236 del 2001 dell'Autorità di garanzia, dal titolo "Regolamento per l'esercizio e la tenuta del registro degli operatori di comunicazione").

Proprio per il fatto che l'obbligo di iscrizione concerne indiscriminatamente tutti gli operatori della comunicazione, comprese le imprese fornitrici di servizi telematici e di telecomunicazioni, deve ritenersi che esso riguardi anche i fornitori di accesso ad Internet (ed anche i provider di primo livello). La stessa delibera istitutiva del roc ha peraltro precisato che per "imprese fornitrici di servizi di telecomunicazioni e telematici", che risultano tra i soggetti destinatari dell'obbligo di iscrizione al registro, si intendono "i soggetti che, in base a licenza o autorizzazione, installano e forniscono reti di telecomunicazione o forniscono servizi consistenti, in tutto o in parte, nella trasmissione e nell'instradamento di segnali su reti di telecomunicazioni". Più recentemente, a seguito del riassetto operato dall'appena citato codice delle comunicazioni elettroniche, è stato ribadito che tutti i soggetti titolari di autorizzazione del ministero delle comunicazioni all'esercizio dei servizi di comunicazione elettronica siano tenuti all'iscrizione nel roc (appunto art. 25, comma 4).

Deve infine ricordarsi come, con la legge n. 59 del 2002, sia stata presa in considerazione dal legislatore specificamente l'attività degli internet provider (intesi quali fornitori di accesso alla rete), ai fini della loro equiparazione agli operatori telefonici per quanto riguarda la fruizione delle condizioni economiche tariffarie.

Ancor più di recente, l'attività dei fornitori di accesso ad Internet è stata oggetto della delibera dell'Autorità per le Garanzie nelle Comunicazioni (n. 131 del 2006), con la quale l'autorità, nell'esercizio dei poteri conferiti dalla legge, ha stabilito, anche in un ottica di protezione dei diritti dei consumatori e degli utenti, adeguati livelli dei servizi forniti dai provider in esame ed ha previsto anche un sistema di indennizzi automatici, in caso di interruzioni e malfunzionamenti dei servizi stessi.

---

[17] Ciò sia perchè una cosa è la disciplina pubblicistica (amministrativa), che regola l'accesso alla fornitura del servizio, in quanto collegata alla gestione di un servizio di interesse pubblico, altro è la disciplina privatistica, attinente cioè ai rapporti tra i soggetti che hanno ottenuto l'autorizzazione ed i loro clienti finali, sia perchè la disciplina prevalentemente privatistica, contenuta nel d.lgs. 70/2003 di recepimento della direttiva comunitaria sul commercio elettronico, riguardando l'assetto giuridico dei rapporti tra prestatori e destinatari dei servizi della società dell'informazione, vale a dire, sostanzialmente, delle attività economiche on-line, non può che attenere anche all'attività svolta dai fornitori di accesso alla rete nei confronti dei loro clienti e dei loro potenziali clienti (più chiaramente, il provider che fornisce servizio di accesso ad internet o di web hosting, anche a seguito di contratti stipulabili on-line, deve fornire tutte le informazioni obbligatoriamente previste dal d.lgs. 70/2003 ai destinatari dei suoi servizi).

Volendo quindi verificare se le disposizioni definitorie relative agli attori del commercio elettronico, contenute nel d.lgs. 70/2003, siano rispondenti all'odierna fase di sviluppo delle attività in rete, può dirsi sinteticamente quanto segue.

Al di là della definizione unitaria, e solo apparentemente onnicomprensiva di prestatori di ssi sulla base del minimo comune denominatore dello svolgimento di attività latamente economiche , contenuta nell'art. 2 d.lgs. 70/2003, essa qualifica soggetti dalle attività molto diverse: dagli intermediari necessari dei servizi della società dell'informazione (appunto access, caching ed hosting provider), ai prestatori che svolgono quello specifico servizio della società dell'informazione che è il commercio elettronico, attraverso l'offerta di beni e servizi, a quegli ulteriori prestatori che, pur non svolgendo attività economica diretta, effettuano attività – peraltro sempre più diffuse - mediante le quali rendono accessibili dati ed informazioni (motori di ricerca, wikipedia, gestione di piattaforme ugc, social networks, etc.), comunque economicamente valutabili.

Per quanto attiene alla definizione di "destinatario del servizio", proprio in considerazione dello sviluppo degli aggregatori di contenuti, stimolati proprio dall'attività di uploading degli utenti, pare che la attività consistente nel "rendere accessibili informazioni", prevista dall'art. 2, lett. d), come una di quelle che identificano il destinatario del servizio, stia assumendo un ruolo sempre più rilevante e non meramente residuale rispetto a quello di "ricerca" delle informazioni, sia essa finalizzate all'acquisto che, più semplicemente, alla mera acquisizione di conoscenza.

3. Profili della contrattazione a conclusione telematica.

Come si già accennato nel primo paragrafo, uno degli aspetti del dibattito circa l'opportunità di adottare nuove regole privatistiche per disciplinare lo svolgimento di attività giuridica mediante l'uso della information technology ha interessato proprio l'ambito della contrattazione telematica.

Si tratta di un profilo di rilevanza centrale, considerato che l'e-commerce in senso stretto può essere descritto proprio come quell'insieme di relazioni contrattuali, aventi ad oggetto l'acquisto di beni o servizi, che si instaurano tra soggetti mediante l'uso di strumenti telematici.

Da questo punto di vista, alla luce del diritto italiano, la contrattazione telematica rappresenta un ulteriore sviluppo delle tecniche di conclusione del contratto inter absentes (vale a dire tra soggetti che si relazionano senza essere contemporaneamente presenti in un medesimo luogo fisico) rispetto a quelle che avevamo conosciuto anche in epoca recente (si pensi, ad esempio, alla conclusione del contratto a mezzo telefax).

Ciononostante, la novità rappresentata dalle modalità telematiche di espressione della volontà negoziale è stata tale da originare un dibattito intorno alla validità stessa dei contratti stipulati per mezzo dell'elaboratore.

La difficoltà non consisteva tanto nel fatto che nei contratti a conclusione telematica l'accordo non venisse raggiunto tra persone presenti, dato che già lo stesso codice civile contempla l'ipotesi che il contratto possa perfezionarsi tra persone "lontane", come risulta dallo stesso

schema delineato dall'art. 1326 c.c., secondo il quale il contratto è concluso nel momento in cui colui che ha fatto la proposta ha conoscenza dell'accettazione dell'altra parte, quanto nel fatto che il procedimento formativo immaginato in tali ipotesi dal legislatore del 1942 è basato su uno scambio, in tempi che possono anche essere successivi, e non contestuali, di dichiarazioni di volontà (proposta e accettazione) "scritte", che, per giunta, si presumono conosciute allorchè pervenute all'indirizzo del destinatario (come risulta dall'art. 1335 c.c.). Ci si è pertanto domandati, in un primo momento, se tale sistema di perfezionamento dell'accordo tra persone fisicamente non compresenti, potesse reggere anche di fronte a modalità comunicative della volontà assolutamente sconosciute all'epoca della redazione del codice civile; si trattava quindi di verificare se lo schema risultante dal combinato disposto degli artt. 1326 e 1335 c.c. fosse compatibile con lo scambio telematico di dichiarazioni di volontà (proposta e accettazione), compatibilità che avrebbe richiesto, come presupposto, l'equiparazione delle dichiarazioni on-line alle più tradizionali comunicazioni effettuate per iscritto (appunto una proposta inviata per posta e sottoscritta con firma autografa, alla quale facesse seguito una accettazione spedita al proponente nella medesima forma)[18].

E' allora evidente come, in questo quadro, assumesse una importanza centrale, per l'esistenza stessa del commercio elettronico, l'inequivoco riconoscimento della validità dei contratti telematici (per meglio dire contratti a conclusione telematica).

Al fine di sgombrare il campo da ogni dubbio al riguardo, si sono registrati una serie di importantissimi interventi da parte del legislatore italiano, taluni di diretto impulso interno, altri di derivazione comunitaria, in quanto contenuti in atti normativi di recepimento di direttive, il cui esito ultimo e, in certo senso, definitivo, è rappresentato dal Codice dell'amministrazione digitale (d.lgs. n. 82 del 2005)[19].

---

[18] Le modalità telematiche di formazione dell'accordo pongono anche altre questioni, come ad esempio quelle relative alla identificabilità dell'autore della dichiarazione, alla integrità e inalterabilità della dichiarazione stessa, alle condizioni alle quali ritenere avvenuta la trasmissione e la ricezione della dichiarazione, rispetto alle quali l'unica garanzia, alla luce della normativa vigente, è rappresentata dall'utilizzazione di documenti informatici sottoscritti con firma digitale o altro tipo (ad oggi non tecnicamente presente sul mercato) di firma elettronica qualificata.

[19] I contributi dottrinari in tema di documento informatico e firma digitale, succedi tisi negli anni a far data dalla introduzione nel nostro ordinamento della firma digitale, sono numerosissimi. In questa sede mi limito a citare GENTILI, I documenti informatici, Validità ed efficacia probatoria, in Dir. internet, 2006, 3; BUONOMO, Processo telematico e firma digitale, Milano, 2004; FINOCCHIARO, Firma digitale e firme elettroniche. Profili privatistici, Milano, 2003. Volendo svolgere un sintetico excursus sull'evoluzione della disciplina italiana in tema di documento informatico e firme elettroniche, può osservarsi quanto segue. Il primo dei molteplici interventi è rappresentato dall'art. 15, II comma, della legge 15 marzo 1997, n. 59, meglio nota come "Bassanini 1", il quale stabilisce che "gli atti e i documenti formati dalle pubbliche amministrazioni e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonchè la loro archiviazione e trasmissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge". Successivamente, l'art. 11, n. 1 del d.p.r. n. 513 del 1997 (decreto con il quale venivano individuate le modalità concrete di attuazione del principio generale enunciato nell'appena citato art. 15 l. 59/1997), ha riconosciuto validità e rilevanza, "a tutti gli effetti di legge", ai contratti stipulati con strumenti informatici o per via telematica "mediante l'uso della firma digitale", e tale enunciato è stato poi trasfuso nell'art. 11 del d.p.r. n. 445 del 2000, nel quadro del più generale principio della rilevanza e validità dei documenti informatici, enunciato nell'art. 8. Un ulteriore, importantissimo riconoscimento della validità dei contratti stipulati in via telematica risulta dal d.lgs. 185 del 1999 (di recepimento della direttiva comunitaria 97/7 in materia di contratti a distanza, ora trasfuso nel codice del consumo), il quale qualifica come "tecnica di comunicazione a distanza", "qualunque mezzo che, senza la presenza fisica e simultanea del fornitore e del consumatore, possa impiegarsi per la conclusione del contratto" (art.1, lett. d): è di tutta evidenza come questa definizione si attaglino perfettamente alle modalità di contrattazione

Il legislatore europeo, da parte sua, ha ritenuto che l'utilizzazione dello strumento telematico

che avvengono nel commercio elettronico e come la previsione legislativa di una disciplina ad hoc per la "categoria" dei contratti "a distanza" non faccia che ribadirne la validità.Altra conferma della validità dei contratti telematici si trae dall'art. 13 del d.lgs. 70/2003, I comma, il quale stabilisce che "le norme sulla conclusione dei contratti si applicano anche nei casi in cui il destinatario di un bene o di un servizio della società dell'informazione inoltri il proprio ordine per via telematica". Da questa enunciazione derivano due importanti conseguenze: a) i contratti possono essere conclusi per via telematica e, quindi, come abbiamo sinora detto, non possono che essere validi; b) la modalità telematica di incontro delle volontà non incide sulle norme di diritto comune, contenute nel codice civile, sulla conclusione dei contratti, le quali restano quindi perfettamente compatibili anche con la contrattazione telematica (la differenza consiste soltanto nel fatto che, come si vedrà in seguito – paragrafo 4 del III capitolo - l'intera fase prodromica alla vera e propria conclusione del contratto è caratterizzata dall'imposizione di una serie di obblighi, incombenti sul soggetto che offre on line beni o servizi, integrativa della disciplina tradizionale della conclusione del contratto contenuta nel codice civile e delle normative settoriali di protezione dei consumatori).
Quanto finora detto circa la validità dei contratti telematici, espressamente o implicitamente risultante dai testi normativi menzionati, non può certo stupire, se si pensa che nel nostro ordinamento il requisito principale del contratto è l'accordo, comunque manifestato, e ciò in ossequio al principio della libertà delle forme, vale a dire di libertà del mezzo sociale attraverso il quale le parti manifestano il loro consenso (l'accordo, e quindi il contratto, avente il contenuto richiesto dall'art. 1321 c.c., può esservi manifestato con atto pubblico, con scrittura privata, in forma orale, come pure con un comportamento materiale).
Nelle contrattazioni tradizionali, pur ispirate al principio appena detto, assume un importantissimo rilievo l'attività di documentazione del contratto, intesa nel senso di attività idonea ad attribuire ad una cosa una capacità rappresentativa. Si è conseguentemente posto il problema di individuare regole che consentano ai documenti informatici, vale a dire alle rappresentazioni informatiche di atti o fatti giuridicamente rilevanti, di garantire le medesime funzioni proprie dei documenti cartacei, così da far sì che il documento informatico potesse assolvere alle due funzioni giuridiche riconosciute ai documenti cartacei: quella di valida costituzione dei rapporti giuridici (ed è l'aspetto del regime normativo del documento che attiene alla forma, ove prevista dalla legge sotto pena di nullità) e quello di dimostrazione, di certezza giuridica dei rapporti (ed è l'aspetto del regime normativo che attiene alla prova).
Tale attività di posizione di regole ad hoc pare essersi di recente, finalmente, stabilizzata, a seguito della pubblicazione di uno dei decreti integrativi al codice dell'amministrazione digitale. Si è forse compiuto quel processo di regolamentazione del documento informatico che ha avuto inizio nel 1997 e che è poi proseguito con successivi interventi modificativi, talvolta di derivazione interna, talaltra comunitaria, che non hanno certo facilitato l'attività degli interpreti. Pur nella differenza delle formulazione adottate nei vari interventi susseguitisi, risulta evidente che la disciplina legislativa del documento informatico si è sempre sviluppata su un duplice piano: quello della rilevanza (validità) sostanziale del documento (questione che si risolve nel rapporto tra forma "informatica" e forma scritta) e quello dei suoi effetti probatori. Il tutto nel quadro del generale principio della validità e rilevanza del documento informatico, a tutti gli effetti di legge, anche quando non sottoscritto.
Tale situazione si riscontra anche nella disciplina attualmente vigente. Innanzitutto, il I comma dell'art. 20 del cod. amm. dig. (intitolato "Documento informatico") conferma, pur con qualche variazione letterale, il principio generale, più volte enunciato in precedenza, della rilevanza e validità dei contratti telematici, laddove stabilisce che "il documento informatico da chiunque formato, la registrazione 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".
La disposizione prosegue, poi, disciplinando il primo dei due piani sui quali si articola la disciplina del documento informatico: quello dei requisiti che il documento informatico deve possedere affinché possa soddisfare il requisito legale della forma scritta, ai fini della sua validità. Il secondo comma dell'art. 20 prevede, infatti, che il documento informatico sottoscritto con firma digitale o con firma elettronica qualificata, formato nel rispetto delle regole tecniche stabilite ai sensi dell'art. 71 del codice stesso, soddisfa il requisito della forma scritta, anche nei casi previsti, sotto pena di nullità, dall'art. 1350 c.c.
Di recente, però, con l'aggiunta effettuata dal decreto legislativo n. 159 del 2006, integrativo del Codice dell'amministrazione digitale, si è inteso aumentare la possibilità di riconoscere il requisito della forma scritta anche quando non si utilizzino i meccanismi di sottoscrizione più rigorosi, quali sono appunto quello della firma digitale e degli altri tipi di firma elettronica qualificata, in quanto è stato inserito nel Codice amministrazione digitale, all'art. 20, un comma 1-bis, nel quale è previsto che, fermo restando quanto stabilito dall'appena descritto II comma, l'idoneità del documento informatico a soddisfare il requisito della forma scritta sia liberamente valutabile in giudizio, tenuto contro delle caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità del documento medesimo.
Il successivo art. 21 (intitolato "Valore probatorio del documento informatico sottoscritto") del Codice dell'amministrazione digitale è invece rivolto a disciplinare il secondo dei due piani sopra ricordati: quello della prova. In

per la contrattazione non presentasse elementi di specificità tali da rendere necessario un intervento normativo che andasse a differenziarne la disciplina rispetto al contratto di diritto comune.

Prova ne sono il considerando n. 34, secondo il quale gli stati membri dovrebbero adeguare le parti della propria legislazione relative soprattutto ai requisiti di forma che potrebbero ostacolare il ricorso ai contratti per via telematica, al fine di renderli possibile e validi e, soprattutto, l'art. 9, primo comma, della direttiva, il quale impone agli stati membri di provvedere affinchè "il loro regolamento giuridico renda possibili i contratti per via elettronica e di assicurare che la normativa sulla formazione del contratto non sia di ostacolo all'uso effettivo dei contratti elettronici e non li privi di validità ed efficacia".

Conseguentemente, come è noto, la disposizione italiana di recepimento sul punto, precisa espressamente, al primo comma dell'art. 13 d.lgs. n. 70 del 2003, che le norme italiane sulla conclusione dei contratti si applicano anche quando l'accordo venga raggiunta utilizzando gli strumenti telematici.

Questo significa che la conclusione di un contratto in via telematica continua ad essere tranquillamente disciplinata dalle regoli generali contenute nel nostro codice civile.

Se ciò è vero, è altrettanto vero che il legislatore comunitario prima, e quello interno poi, hanno introdotto talune disposizioni che, senza affatto incidere sulle regole esistenti in tema di conclusione dei contratti, le hanno corredate di talune previsioni ulteriori, finalizzate ad adeguare la disciplina comune alla particolarità del mezzo tecnologico utilizzato per la veicolazione delle dichiarazioni di volontà (il riferimento, come noto, è alla introduzione di obblighi informativi precontrattuali e in corso di contratto gravanti sul prestatore del servizio, parte forte del rapporto, in sostanziale analogia con le regole elaborate dal legislatore europeo in tema di contratti dei consumatori e, soprattutto, a quello, del tutto innovativo, della previsione di un obbligo del prestatore di "accusare ricevuta" dell'ordine di acquisto ricevuto dal cliente (destinatario del servizio, secondo la terminologia del legislatore del d.lg. n. 70 del 2003)[20].

Alla luce di quanto detto, si può tranquillamente affermare che attualmente non sussistono dubbi sulla validità ed efficacia dei contratti a conclusione telematica, come pure sul fatto che tale conclusione avvenga secondo le regole di diritto privato comune, integrate da quelle previste dal d.lgs. n. 70 del 2003 e, eventualmente, da quelle ulteriori, contenute in altri testi

particolare, il suo II comma prevede che soltanto ai documenti sottoscritti con firma digitale o con altro tipo di firma elettronica qualificata, venga attribuita l'efficacia probatoria prevista dall'art. 2702 c.c. (vale a dire quella della scrittura della privata).

Il regime degli effetti in tema di prova è completato dal primo comma dell'art. 21 del d.lgs. 82/2005, il quale stabilisce l'efficacia probatoria dei documenti informatici sottoscritti con firma elettronica (cosiddetta "semplice", in quanto non digitale, nè effettuata con altro meccanismo di firma qualificata), affermandone la libera valutabilità in giudizio, tenuto conto delle loro caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità.

[20] Giova rammentare che la nozione di"destinatario del servizio", controparte del prestatore-contraente forte nel rapporto contrattuale on line, è più ampia di quella di consumatore, con chiara conferma della propensione del legislatore comunitario a perseguire una protezione del contraente debole in generale, che prescinda dalla sua qualifica in termini di consumatore secondo la legislazione europea (limitata, come noto, alla sola "persona fisica" che agisca al di fuori dell'attività professionale eventualmente svolta).

normativi ed espressamente richiamate dal medesimo decreto di recepimento della direttiva[21].

Ciò premesso, risulta possibile tracciare un quadro sintetico di come in questi anni sia stata affrontata la tematica della contrattazione on line e di quali siano, ad oggi, le questioni che ancora suscitano discussioni e perplessità.

3.1. Il contratto "point and click" e la teoria dello scambio senza accordo.

La stragrande maggioranza dei contratti conclusi sulla rete internet avviene secondo la modalità c.d. point and click, con la quale si descrive la condotta del destinatario del servizio il quale prima "punta" il mouse sulla zona di interesse (corrispondente al bene o servizio richiesto, sulla quale è solitamente presente l'espressione "acquisto" o quella "accetto") presente all'interno del negozio virtuale e poi – pressoché contestualmente – effettua una digito-pressione sullo stesso, con la quale manifesta la volontà di concludere il contratto avente ad oggetto quel bene o quel servizio[22]. Tale modalità comportamentale dell'acquirente on line, secondo autorevole dottrina[23], farebbe decadere il rapporto contrattuale tra prestatore e destinatario del servizio a mero scambio senza accordo, non coincidente con quello di cui all'art. 1321 c.c., che proprio sul concetto di accordo è incentrato. Si tratta, come è noto, anche alla luce del dibattito dottrinario al quale questa ricostruzione ha dato luogo, di una teoria che evidenzia la realtà effettiva degli scambi nell'odierna realtà della produzione seriale e degli scambi di massa, nella quale svanisce quel momento dialogico del contratto di cui erano espressione le trattative e la comune costruzione del regolamento che caratterizza l'accordo: in assenza di tali caratteri, non si potrebbe più parlare di accordo, visto che la volontà del destinatario del prodotto verrebbe ad essere ridotta "all'elementare libertà di non compiere l'atto". Nella nuova fase dello scambio capitalistico, caratterizzata dall'impiego di tecniche che si basano su una sorta di meccanica ritualità, che consente all'imprenditore di operare in modo più rapido, razionale, e quindi efficiente economicamente, al contratto inteso come accordo, ai sensi degli artt. 1321 e 1325 c.c., se ne affiancherebbe un altro, nel quale l'accordo viene sostituito da atti unilaterali che non dichiarano alcunché, ma si limitano ad esporre virtualmente merci, da un lato e, dall'altro, ad acquisirle, semplicemente scegliendole con l'impiego del mouse[24].

Alla così descritta teoria dello scambio senza accordo, dalla cui accettazione deriverebbe la conseguenza della sottrazione a tali scambi della disciplina generale del contratto (con conseguente inapplicabilità delle norme sui rimedi e di quella sulla protezione del consumatore)

---

[21] Si tratta, soprattutto, dei rinvii operati all'ex 185 del 1999, in tema di contratti a distanza, attualmente trasfuso all'interno del Codice del consumo (d.lgs. n. 206 del 2005).

[22] Ciò in linea di massima in quanto, come si sta per dire, la condotta del destinatario del servizio può essere anche oggetto di differente qualificazione, a seconda degli elementi rappresentati al pubblico nella vetrina virtuale.

[23] IRTI, Scambi senza accordo, in Riv. trim. dir. Proc. Civ., 1998, 347 e 360, il quale parla anche, a tale proposito, di un contrahere senza consentire.

[24] Così IRTI, Scambi senza accordo, cit., 302.

è stato replicato, altrettanto autorevolmente, che l'art. 1321 non postula necessariamente il dialogo o la trattativa, bensì la sola convergenza di due dichiarazioni unilaterali, quella di proporre e quella di accettare, dichiarazioni di manifestazione di volontà che non devono peraltro far ricorso alla parola, scritta o proferita, ma possono essere sostituite da comportamenti concludenti[25].

Si tenga presente che quanto viene perduto a livello di trattativa viene però recuperato, in un'ottica di protezione del destinatario del servizio quale contraente debole (che non coincide necessariamente con la figura di consumatore, avendo un ambito oggettivo più ampio)[26].

Esulano, ovviamente, dalla problematica descritta, i contratti conclusi a seguito di incontro tra proposta ed accettazione a seguito di scambio di e-mail, in quanto esse riproducono, mediante l'utilizzazione di strumento comunicativo diverso dalla voce e (tendenzialmente) dallo scritto[27], la fase delle trattative, tanto è vero che talune disposizioni del d.lgs. n. 70 del 2003 relative agli obblighi informativi e quelle all'obbligo del prestatore di accusare ricevuta dell'inoltro dell'ordine, per previsione espressa, non trovano applicazione ai contratti conclusi via e-mail.

Questa tecnica generale di conclusione del contratto, risultante dal combinato disposto degli artt. 1326 e 1335 c.c. nel quadro del commercio elettronico, trova applicazione nelle contrattazioni individualizzate, vale a dire effettuate tra soggetti determinati, destinatari della proposta e della accettazione; si tratta di una modalità che si realizza soprattutto via e-mail e che può derivare sia da una precedente conoscenza tra i soggetti che entrano in contatto sia al di fuori di ogni precedente relazione, come avviene allorchè un operatore economico invii una proposta, mediante e-mail, a potenziali clienti, ognuno nominativamente individuato grazie alla utilizzazione di indirizzari e-mail spesso distinti in categorie grazie alle note attività di profilazione dei consumatori. In questo caso, come si è accennato, opererà il principio della conoscibilità dell'accettazione, con la conseguenza che il contratto si considererà concluso nel momento in cui l'accettazione, ovviamente conforme alla proposta, giunge nel "recipiente" dei messaggi del provider del proponente, configurando questo l'indirizzo del proponente stesso. Una conferma di ciò deriva anche dal disposto dell'art. 45 del Codice dell'amministrazione digitale (intitolato "Valore giuridico della trasmissione"), il quale, al II comma, prevede testualmente che "il documento informatico trasmesso per via telematica si intende spedito dal mittente se inviato al proprio gestore, e si intende consegnato al destinatario se reso disponibile all'indirizzo elettronico da questi dichiarato, nella casella di posta elettronica del destinatario messa a disposizione dal gestore". Questo schema di conclusione del contratto può trovare applicazione, secondo parte della dottrina, anche al di fuori della utilizzazione di e-mail (e quindi di rapporti che nascono individualizzati), in quanto potrebbe operare nei casi in cui i siti di e-

---

[25] E' questa la posizione di OPPO, Disumanizzazione del contratto?, in Riv. dir. civ., 1998, I, 528 e ss; a tali osservazioni ha poi replicato RTI, "E' vero, ma … " (replica a Giorgio Oppo, in Riv. dir. civ., 1999, I, 273.
Su tali problematiche, si veda di recente in dottrina AZZARRI, La conclusione dei contratti telematici nel diritto privato europeo, in Contratti, 2010, 301.

[26] Sul punto, si veda in dottrina AZZARRI, La conclusione, cit., 304; MANNA, ….

[27] Ciò in quanto l'equiparazione del documento informatico con quello scritto, cartaceo, si ha solo in presenza di documento sottoscritto mediante firma digitale, mentre la dichiarazione di volontà espressa mediante mail rappresenterebbe, al più, documento informatico sottoscritto con firma elettronica semplice (o debole).

commerce, i quali solitamente presentano un insieme di mere offerte al pubblico, siano invece strutturati con modalità interattive, tali da consentire una individualizzazione della proposta e, soprattutto, lo svolgimento di trattative, vale a dire la possibilità, per il cliente, di concorrere a determinare il contenuto negoziale[28].

3.2. Point and click e schemi diversificati di conclusione del contratto: offerta al pubblico, invito a proporre, conclusione mediante inizio di esecuzione.

Se la conclusione del contratto "point and click" rappresenta senz'altro quella statisticamente più frequente, se non assolutamente dominante, nel mondo delle relazioni contrattuali internettiane, essa non è però sempre riconducibile al medesimo modello di formazione dell'accordo secondo le regole codicistiche.

La conclusione del contratto può avvenire a seguito di offerta al pubblico ex art. 1336 c.c., in tutti quei casi in cui l'offerta presente on line sia completa di tutti gli elementi essenziali.

Non vi è dubbio che si tratti della più diffusa modalità di conclusione dei contratti on line, sui quali si basa il commercio elettronico. Si ha infatti offerta al pubblico ogni volta che una proposta, indirizzata ad una molteplicità di soggetti indeterminati (alla generalità degli utenti web) contenga tutti gli elementi essenziali del contratto, che quindi, per essere concluso validamente, non abbisogna di null'altro che della accettazione[29].

Si tratta quindi, con evidenza, delle ipotesi (che peraltro sono la stragrande maggioranza nella pratica dell'e-commerce) nelle quali il destinatario del servizio può soltanto aderire o rifiutare quella proposta che gli proviene dal prestatore nella particolare modalità dell'offerta al pubblico, vale a dire di quella ipotesi di proposta diretta non ad un soggetto determinato bensì ad una pluralità indistinta e indeterminata di soggetti. In questi casi il cliente non ha la possibilità di modificare il regolamento contrattuale unilateralmente predisposto dal prestatore, ma può soltanto accettarlo oppure non prenderlo in considerazione[30].

E' noto che l'accettazione interviene in questi casi solitamente mediante la compilazione del form predisposto dall'offerente e la digitazione del tasto virtuale, appunto la cosiddetta moda-

---

[28] E' quanto accade in molti siti, nei quali il prestatore del servizio, effettua sì una proposta, ma consente anche al cliente, attraverso il riempimento di apposite aree o la scelta tra clausole multiple, di effettuare le proprie modifiche e/o richieste, interagendo così con la controparte.

[29] Secondo la dottrina, non viene meno la natura di offerta al pubblico rispetto a quei beni acquistabili on line, il cui prezzo o le cui caratteristiche divengono visibili solo con livelli successivi di consultazione (ad esempio accade che il bene sia in vetrina sul sito, ma il suo prezzo appaia solo dopo aver cliccato sul form "acquisto").

[30] Come accennato sub a), nel caso in cui il sito contenga anche delle modalità interattive, si dovrà verificare se ciò comporti l'esistenza di effettive trattative, incompatibili con l'offerta al pubblico, oppure se, nonostante l'esistenza di una limitata possibilità di determinare il contenuto del contratto, si resti in presenza di un'offerta al pubblico, quanto meno sotto forma di possibilità di scelta dell'utente tra una pluralità di coesistenti proposte contrattuali in incertam personam.

lità "point and click", con la quale si verifica la previsione normativa dell"inoltro dell'ordine", secondo la terminologia adottata dall'art. 13 d.lgs. n. 70 del 2003, la quale integra appunto accettazione di una proposta contrattuale formulata in internet nella modalità dell'offerta al pubblico[31]. La conclusione del contratto avviene pertanto nel momento in cui gli impulsi elettronici, sui quali transita l'accettazione vengono registrati dal server del provider del proponente, come risulta dal disposto dell'art. 13, comma 3, d.lgs. n. 70 del 2003, secondo il quale l'ordine si considera pervenuto quando il destinatario ha la possibilità di accedervi[32].

Rispetto a tale modalità, ci si è domandati cosa accade nel caso in cui il proponente non sia in grado di soddisfare tutte le richieste che gli siano pervenute, in quanto gli ordini sopravanzano i beni materialmente disponibili; si tratta di una problematica di non agevole soluzione. Da una parte, infatti, si ritiene che in tale ipotesi debbano essere soddisfatti gli ordini secondo un criterio generale di priorità temporale, con la conseguenza che saranno soddisfatti, sino ad esaurimento della merce, coloro che per primi abbiano accettato quella particolare forma di proposta che è l'offerta al pubblico [33]. Si ritiene altresì che, nel caso in cui il proponente non avesse dato notizia sul sito della limitata disponibilità dei beni offerti, e questa non fosse desumibile ragionevolmente dalla natura del beni, egli dovrebbe rispondere a titolo di responsabilità contrattuale per inadempimento, dato che l'inoltro dell'ordine, rappresentando accettazione della proposta e, pertanto, conclusione del contratto, aveva fatto sorgere l'obbligo di consegnare il bene compravenduto[34]. Deve però a tale proposito specificarsi che, in considerazione del fatto che l'art. 54, comma secondo, del Codice del consumo, prevede che ove la mancata esecuzione sia dovuta alla indisponibilità, anche temporanea, del bene o del servizio richiesto, il professionista possa liberarsi dal vincolo dando notizia dell' inconveniente al consumatore nel termine previsto dal primo comma di quello stesso articolo, provvedendo a rimborsargli le spese eventualmente già sostenute, così però, di fatto, vanificando il diritto del creditore all'adempimento e finendo per beneficiare di una sorta di recesso[35].

Accade però spesso che il prestatore del servizio della società dell'informazione, titolare del sito di e-commerce, non intenda restare vincolato in anticipo alla sua proposta, come avviene nell'ipotesi della proposta (offerta) al pubblico, o comunque voglia riservarsi la possibilità di scegliere la propria controparte. In tali casi predispone, sul sito, una offerta che non contiene tutti gli elementi di una proposta e che quindi non può valere come tale: si è allora in presenza di quello che la dottrina qualifica come invito ad offrire o invito a proporre[36]. Ciò comporta che i "ruoli" delle parti finiscano per essere invertiti: l'acquirente, completando la "proposta", diviene proponente ed il titolare del sito si trova così nella posizione di accettante, ed ha, di

---

[31] In tal senso, in dottrina, PENNASILICO, La conclusione dei contratti on line tra continuità e innovazione, in Dir. Inf., 2004, 825; PERLINGIERI G., Il contratto telematico, in VALENTINO (a cura di), Manuale di diritto dell'informatica, Napoli, 2004, 40.

[32] MANNA, La disciplina del commercio elettronico, cit., 142; AZZARRI, La conclusione, cit., 310,

[33] Così afferma AZZARRI, La conclusione, cit., 308.

[34] In questo senso ancora AZZARRI, La conclusione, loc. ult. cit.

[35] Cfr, ancora AZZARRI, loc. ult. Cit.; GRISI, Lo "ius poenitendi" tra tutela del consumatore e razionalità del mercato, in Riv. crit. dir. priv., 2001, 604.

[36] Cfr., in tal senso, MANNA, La disciplina, cit., 95.

fatto, in questo modo, la possibilità di riservarsi di concludere il contratto.

E' evidente che, nelle ipotesi di invito ad offrire, il contratto risulta concluso nel tempo e nel luogo in cui l'impulso elettronico che veicola l'accettazione viene immagazzinato sul server del provider del cliente, destinatario della proposta originariamente incompleta.

E' altrettanto evidente come la qualificazione di un'esposizione di beni o servizi on line come offerta al pubblico o come invito ad offrire vada effettuata alla luce di un esame del contenuto effettivo delle dichiarazioni, non avendo alcuna rilevanza la qualificazione formale eventualmente indicata dalle parti (ciò in quanto generalmente il prestatore-fornitore del bene tende talvolta a qualificare espressamente come inviti a proporre quelle che sono, a tutti gli effetti, delle vere e proprie offerte al pubblico).

In dottrina, sulla base della constatazione che nella prassi delle contrattazioni on line è molto frequente la richiesta, fin dalla compilazione del modulo d'ordine, di digitazione del numero di carta di credito, è stata avanzata, rispetto a tali casi, la teoria della utilizzabilità dello schema di conclusione del contratto previsto dall'art. 1327 c.c., in considerazione della possibilità di interpretare l'invio del numero di carta di credito come inizio di esecuzione[37].

Come è noto, l'art. 1327 c.c. prevede che qualora, su richiesta del proponente, o per la natura dell'affare o in base agli usi, la prestazione debba effettuarsi senza una preventiva risposta, il contratto è concluso nel luogo e nel tempo nei quali ha avuto inizio l'esecuzione, purchè sia successiva e conforme alla proposta. Ebbene, la dottrina non è concorde circa l'attribuibilità di valore di esecuzione alla digitazione e invio dei dati della propria carta di credito, soprattutto in considerazione della di[38].

Secondo una prima impostazione, digitazione ed invio dei dati indicati, in quanto finalizzati a garantire immediatamente il pagamento del bene o del servizio, anzi, addirittura ad effettuarlo, dovrebbero valere come inizio di esecuzione[39].

Secondo altra opinione, ciò non sarebbe condivisibile per due ordini di ragioni. Intanto perchè nella prassi di formazione dei contratti on line, nella maggior parte dei casi, la digitazione degli estremi della carta di pagamento è contestuale alla digitazione di tasti di accettazione (cliccata sul form "accetto" , "acquisto" o simili) o, meglio ancora la segue, con la conseguenza che il contratto, nonostante la comunicazione dei dati della carta di pagamento, risulta comunque concluso secondo lo schema classico del pervenimento dell'accettazione della proposta nella forma dell'offerta al pubblico, già descritto[40]. In secondo luogo perchè si ritiene che la comunicazione dei dati della carta non possa essere equiparata ad un inizio di esecuzione, in

---

37 In questo senso, in dottrina,MANNA, La disciplina, cit., 96.

38 Giova precisare come attualmente, nell'ambito dell'e-commerce, siano utilizzabili altre modalità di pagamento ben più veloci, più sicure, in quanto basate su sistemi di crittografia, oltre che capaci di garantire l'anonimato del soggetto, anche al fine di evitare la tracciabilità delle sue operazioni economiche.

39 E' questa l'impostazione di GAMBINO A.M., L'accordo telematico, Milano, 1997, 193; PASQUINO, Servizi telematici e criteri di responsabilità, Milano, 2003, nota 65.

40 Il rilevo, condivisibile, è di PENNASILICO, La conclusione dei contratti on line tra continuità e innovazione, in Dir. inf., 2004., 823; TARICCO, Volontà e accordo nella contrattazione telematica, in Nuova giur. Civ. comm., 2003, II, 218. In senso sostanzialmente analogo, BENEDETTI A.M., Autonomia privata procedimentale. La formazione del contratto tra legge e volontà delle parti, Torino, 2002, 407 e ss.

quanto non si ha pagamento, nè rilascio di un mezzo di pagamento, bensì mera autorizzazione a riscuotere presso l'emittente della carta in conseguenza di una già avvenuta accettazione da parte del destinatario del servizio (cliente)[41].

E' stato ritenuto che tale ultima critica, pur se condivisibile, possa però essere superata ove si facesse ricorso alla moneta elettronica, che in base alla direttiva 2000/46/CE (recepita con l. 1° marzo 2002, n. 39), è da ricomprendere tra i mezzi di pagamento accettati da imprese diverse dall'emittente[42].

3.3. L'obbligo di "accusare ricevuta dell'inoltro dell'ordine", di cui all'art. 13 d.lgs. n. 70 del 2003: natura e funzione.

Come già osservato e come risulta inequivocabilmente dal primo comma dell'art. 13 del decreto di recepimento, le norme sulla conclusione dei contratti si applicano anche ai contratti telematici, con la conseguenza che il contratto on line risulta già concluso al momento in cui, a seguito dell'inoltro dell'ordine da parte del consumatore o dal non consumatore, che rappresa accettazione della proposta formulata, nella modalità dell'offerta al pubblico, da parte del prestatore, tale accettazione perviene al destinatario quando questi ha la possibilità di accedervi (così il terzo comma dell'art. 13)[43]. Ne consegue che l'obbligo del prestatore di "accusare ricevuta" dell'inoltro dell'ordine, in via telematica e senza ingiustificato ritardo, rappresenta allora un elemento estraneo al procedimento formativo del contratto, rientrante come tale tra gli obblighi post-negoziali, in quanto relativo ad un contratto già concluso[44].

Una tale impostazione risulta confermata dal fatto che il legislatore europeo abbia abbandonato

---

41 Così OPPO, Disumanizzazione del contratto?, cit., 529 e ss., il quale non riconosce efficacia solutoria allo strumento di pagamento in questione.

42 Per tale rilievo, si veda AZZARRI, La conclusione, cit., 311. In generale, sulla disciplina della moneta elettronica, può leggersi FINOCCHIARO, Pagamento elettronico e moneta elettronica, in TOSI (a cura di), Commercio elettronico e servizi della società dell'infornazione, Milano, 2003, 229 e ss.

43 A tal proposito, parte della dottrina (PASQUINO, La conclusione del contratto nella direttiva sull'e-commerce, in Il contratto telematico, a cura di Ricciuto e Zorzi, Padova, 2002, 107) ha ipotizzato che si tratti di una presunzione che riecheggia soltanto, senza coincidervi, con quella di cui all'art. 1335 c.c., in quanto sarebbe caratterizzata da carattere assoluto, non essendo espressamente contemplata una prova contraria; altra parte della dottrina (DELFINI, I contratti stipulati per via telematica nei principi acquis del diritto comunitario dei contratti, in DE CRISTOFARO (a cura di), I "principi" del diritto comunitario dei contratti. Acquis communautaire e diritto privato europeo, Torino, 2009, 183.
Giova ricordare come questa previsione, oltre a poter essere oggetto di deroga quando nessuna delle parti sia un consumatore, non trovi applicazione quando il contratto sia stato concluso a seguito di scambio di e-mail, in quanto come già accennato nel testo lo scambio di posta elettronica dovrebbe comunque garantire il riequilibrio informativo tra le parti e consentire al destinatario del servizio una conoscenza adeguata dell'affare in itinere.

44 Mi limiterò soltanto a dire che secondo taluno, l'invio della ricevuta dell'ordine potrebbe anche configurare accettazione rispetto alla proposta formulata dal destinatario del servizio, in accoglimento dell'invito ad offrire (o a proporre) proveniente dal commerciante elettronico.
In questa ottica avrebbe un senso l'obbligo dell'invio della ricevuta, visto che altrimenti si potrebbe ritenere che il consumatore rischierebbe di venire in possesso di una serie di informazioni, per la prima volta, a contratto già concluso.

il progetto iniziale, contenuto nell'art. 11 della proposta di direttiva presentata alla Commissione il 23 dicembre 1998, il quale introduceva un meccanismo formativo nuovo, il cui momento conclusivo era rappresentato dalla conferma, da parte del prestatore al destinatario, del ricevimento dell'accettazione, nell'ambito di una sequenza che dallo schema classico proposta-accettazione facesse transitare ad uno proposta-accettazione-ricevuta dell'accettazione[45].

Ciononostante, anche alla luce del testo vigente della direttiva e, soprattutto, dell'art. 13 d.gsl. n. 70 del 2002, continuano a rinvenirsi in dottrina interpretazioni volte a valorizzare il ruolo della ricevuta di inoltro dell'ordine nell'ambito dell'iter di perfezionamento del contratto on line.

Secondo una impostazione l'inoltro dell'ordine dovrebbe essere qualificato come una proposta contrattuale e l'invio della ricevuta (come pure l'inizio di esecuzione da parte del prestatore mediante la esecuzione della prestazione) come una accettazione, analogamente a quanto si riscontra nella prassi mercantile di inserire nel contratto clausole quali "salvo approvazione della ditta"[46].

Altra parte della dottrina, in maniera invero singolare ma non condivisibile, sostiene che l'invio dell'ordine non esprimerebbe un'accettazione quanto piuttosto elemento di una fattispecie complessa, composta da ulteriori elementi positivi, quali la dichiarazione di volontà del prestatore e la ricevuta dell'ordine, e da uno positivo, costituito dal mancato esercizio del diritto di recesso nel termine previsto dalla legge[47].

I tentativi di valorizzare, in chiavi di formazione del contratto, la funzione dell'obbligo di trasmissione della ricevuta dell'ordine, sono stati però giustamente criticati, per due ordini di motivi: intanto perchè

non sono compatibili con lo schema tipo dell'offerta al pubblico, il quale rappresenta indubitabilmente il modello prescelto dal legislatore europeo, e confermato da quello italiano, vista la specificazione espressa del fatto che le norme sulla conclusione dei contratti di diritto si applicano anche a quelli a conclusione telematica[48]; inoltre in quanto non appaiono coerenti col dato normativo, in quanto l'obbligo del prestatore di accusare ricevuta dell'inoltro ordine,

---

45 Per tali rilievi si veda MANNA, La disciplina, cit., 133.

46 Per questa impostazione, si veda RICCIUTO, La formazione del contratto telematico e il diritto europeo dei contratti, in RICCIUTO-ZORZI (a cura di), Il contratto telematico, in Trattato di diritto commerciale e di diritto pubblico dell'economia, diretto da Galgano, XXVII, Padova, 2002, 65.

47 Così FOLLIERI, Il contratto concluso in Internet, Napoli, 2005, 130.

48 Per giunta tale impostazione sarebbe difficilmente armonizzabile con la previsione del comma iniziale dell'art. 13, il quale precisa come le norme sulla conclusione dei contratti si applichino anche nei casi di conclusione telematica.
Come potrebbe infatti ritenersi che si applichino le tradizionali norme codicistiche sulla conclusione dei contratti, ove si ritenga che l'accettazione della proposta mediante digitazione del tasto negoziale non sia sufficiente a far sorgere il vincolo, necessitando infatti della conferma di tale accettazione?
La questione, a ben vedere, non è affatto priva di riscontro pratico: se si ritengono operanti le regole codicistiche di cui agli artt. 1326 e 1327 c.c., una volta accettata la proposta, il venditore deve adempiere agli obblighi derivanti dal contratto, ad esempio consegnando il bene acquistato dal consumatore; se invece si ritiene di aderire alla descritta impostazione minoritaria, nessun obbligo sorge, in capo alle parti, prima che il venditore abbia inviato conferma della ricezione dell'ordine all'acquirente, con la conseguenza, però, che viene così ad essere lasciata al venditore l'ultima parola in ordine alla conclusione del contratto nonostante l'avvenuta accettazione da parte del cliente.
Si ritiene quindi che, alla luce del dettato del primo comma dell'art. 13 d. lgs. 70/2003, questa impostazione non possa essere accolta.

unitamente ad un riepilogo delle condizioni generali e particolari del contratto, non fa altro che ripetere quanto già stabilito dall'art. 53, primo comma, del Codice del consumo, in tema di contratti a distanza, il quale prevede che il consumatore debba ricevere conferma delle informazioni previste dalla stessa normativa in tema dei contratti a distanza, prima o al momento della esecuzione del contratto (che quindi risulta, in tal caso, essere già stato concluso)[49].

Ancora, ipotizzare che l'iter formativo del contratto si completi solo allorchè sia decorso il termine per l'esercizio del recesso, come poco sopra si accennava, comporta ulteriori difficoltà, tale da evidenziarne la impraticabilità, visto che non è pensabile legare il completamento del percorso di conclusione del contratto al mancato esercizio di un diritto (quello di recesso, appunto), attribuito soltanto al consumatore in via generale, all'interno di una disciplina, come quella della direttiva 2000/31, la quale ha un ambito soggettivo di applicazione che ricomprende anche i professionisti[50].

Sembra allora maggiormente condivisibile quanto sostiene quella dottrina che, a partire dagli studi di recente sviluppatisi in tema di autonomia privata procedimentale, evidenzia come l'obbligo di accusare ricevuta dell'ordine, corredata delle condizioni contrattuali, non possa che rimanere estraneo al procedimento formativo del contratto, precisando però come proprio l'autonomia privata delle parti ben potrebbe articolare il procedimento di formazione in tre fasi sequenziali:offerta al pubblico (proposta) – inoltro dell'ordine – conferma dell'ordine, attribuendo in tal modo rilevanza procedimentale alla conferma dell'ordine[51].

Nel quadro così descritto, viene da chiedersi per quale motivo sia stato introdotto tale obbligo di accusare ricevuta contenente riepilogo delle condizioni generali e particolari applicabili al contratto, le informazioni relative alla caratteristiche del bene o del servizio e l'indicazione dettagliata del prezzo, dei mezzi di pagamento, del recesso, dei costi di consegna e dei tributi applicabili.

Potrebbe infatti ritenersi che esso risponda all'esigenza di fornire all'utente adeguata informazione riepilogativa sulle condizioni del contratto, sebbene a tal riguardo debba rilevarsi che già da altre disposizioni del d.lgs. n. 70 del 2003 derivano obblighi informativi a carico del prestatore, obblighi che devono essere eseguiti anche prima della conclusione del contratto.

Si pensi a quello del prestatore di fornire le informazioni di cui all'art. 3 d.lgs. 185 del 1999 (ora trasfuso nel Codice del consumo, art. 52), richiamato dall'art. 12 d.lgs. 70/2003, prima dell'inoltro dell'ordine; o ancora al III comma dello stesso art. 12, il quale, con norma inderogabile, prevede che il destinatario del servizio, prima della conclusione del contratto, debba avere a sua disposizione le condizioni generali di contratto in modo che gliene sia consentita la memorizzazione e la riproduzione.

Non solo. Anche l'art. 53 del Codice Consumo (già art. 4 d.lgs. 185 del 1999), che pure trova applicazione al commercio elettronico, stante la clausola generale di salvezza della normativa in materia di protezione dei consumatori contenuta nell'art. 1, terzo comma, d.lgs. n. 70 del 2003, stabilisce che al consumatore debba essere inviata conferma scritta, o su supporto du-

---

[49] Per tali critiche si veda in dottrina AZZARRI, La conclusione, cit., 309.

[50] AZZARRI, La conclusione, cit., 309.

[51] Questa è l'impostazione di BENEDETTI A.M., Autonomia privata procedimentale. La formazione del contratto fra legge e volontà delle parti, Torino, 2002, 407 e ss.

raturo, delle informazioni che coincidono sostanzialmente con quelle oggetto del riepilogo previsto dall'art. 13.

Sembra allora che la ratio della previsione di tale obbligo di accusare ricevuta dell'ordine, corredata del riepilogo delle condizioni del contratto, attenga proprio all'esigenza di integrare la disciplina tradizionale previgente con regole che siano meglio rispondenti alla realtà di svolgimento dei rapporti telematici: visto che la maggior parte dei contratti del commercio elettronico business to consumer vengono stipulati secondo lo schema dell'offerta al pubblico, realizzato mediante la procedura point and click, potrebbe accadere che, nonostante l'assolvimento degli obblighi informativi richiesti al prestatore dagli artt. 7 e 12 in particolare, il consumatore non avesse alcuna documentazione dell'effettiva stipulazione del contratto. L'invio della ricevuta dell'ordine del cliente, con il contenuto riepilogativo indicato, assolve allora ad una funzione di certezza, sia in ordine alla effettiva conclusione del contratto (e ciò sia che si consideri l'inoltro dell'ordine come accettazione di un'offerta, sia che l'ordine stesso venga qualificato come proposta contrattuale formulata in conseguenza dell'invito ad offrire effettuato dal prestatore)[52]. Quasi si volesse fare in modo che il consumatore (o il destinatario) in genere, il quale abbia eventualmente concluso il contratto con un ruolo meramente passivo (come peraltro spesso accade laddove la contrattazione avvenga con il semplice metodo del point and click sul campo "accetto"), senza che egli si sia neppure premurato di valutare le informazioni obbligatorie, possa ottenere un documento riepilogativo degli elementi essenziali dell'operazione contrattuale effettuato, anche in funzione di una sua miglior tutela nella fase successiva alla conclusione.

Per giunta, deve essere evidenziato come la accettazione manifestata mediante digito-pressione del tasto virtuale, pur essendo nei fatti immediata (tanto è vero che la dottrina non ha fatto meno di evidenziare, correttamente, come la contrattazione telematica nella modalità point and click renda di fatto impossibile la revoca dell'accettazione[53]), avrebbe rischiato di far rimanere l'acquirente privo di certezza in ordine al pervenimento della dichiarazione presso il sistema informatico del prestatore, che in tal modo può invece acquisire una "conferma individualizzante" del perfezionamento della relazione instauratasi tra soggetto fino a quel momento privi di rapporto. Tale osservazione ci sembra corroborata dal fatto che l'invio della ricevuta, contenente il riepilogo delle condizioni, debba essere effettuato "senza ingiustificato ritardo" (id est tempestivamente), proprio al fine di evitare che il consumatore (teoricamente, anche il professionista, sebbene rispetto ad esso la norma sia derogabile e l'obbligo di invio dei dati riepilogativi possa essere quindi pretermesso) resti nell'incertezza circa l'avvenuta conclusione del contratto. Oltre a ciò deve essere anche evidenziato come, a ben vedere, i dati riepilogativi comunicati ai sensi del secondo comma dell'art. 13 siano più dettagliati di quelli stabiliti dal"appena ricordato terzo comma dell'art. 12: mentre infatti quest'ultimo menziona, quali informazioni che devono essere fornite dal prestatore prima dell'inoltro dell'ordine da parte dell'acquirente, "le clausole e le condizioni generali del contratto", la ricevuta di cui al

---

[52] Si tratta però di una funzione che, per i motivi già esposti in precedenza, non deve essere confusa con la forma ad probationem, per la quale è comunque richiesta la forma scritta, ottenibile soltanto con il meccanismo della firma digitale di altro tipo di firma elettronica qualificata.

[53] Per tale osservazione si veda, per tutti, AZZARRI, La conclusione, cit., 311.

secondo comma dell'art. 13 contempla anche le condizioni particolari e, soprattutto, l'indicazione del recesso.

Il riferimento appena effettuato al recesso consente di dar conto di una ulteriore teoria in ordine alla funzione dell'obbligo di accusare ricevuta dell'inoltro dell'ordine.

Si è ritenuto infatti che l'invio della ricevuta, corredata delle informazioni prescritte, possa essere considerato come una sorta di condicio iuris, in mancanza dell'avveramento della quale il prestatore del servizio, quand'anche abbia eseguito la propria prestazione, non potrà considerare in mora il destinatario, né computare il decorso del tempo trascorso dall'inoltro dell'ordine ai fini dell'esercizio del recesso[54].

Sotto quest'ultimo profilo, la dipendenza del decorso del termine per l'esercizio del recesso dall'adempimento dell'obbligo di accusare ricevuta contenente le informazioni ex lege stabilite, risulterebbe particolarmente utile rispetto a talune tipologie di contratti, quale quello di assicurazione sulla vita stipulato a distanza, dato che per tale situazione l'art. 11 del recentissimo d.lgs. 190/2005 (ora trasfuso nell'art. 67-duocecies, terzo comma, lett. a), Codice consumo) dispone che il termine di trenta giorni per l'esercizio del recesso decorra dal momento in cui il consumatore "é informato che il contratto è stato concluso".

Infine giova precisare come la menzione del diritto di recesso tra gli elementi che corredano necessariamente la ricevuta dell'ordine debba essere effettuata (o, comunque, possieda effettiva rilevanza) nelle sole ipotesi in cui il prestatore sia un consumatore, in quanto è soltanto nei confronti di questa categoria di soggetti che la legge, in via pressochè generalizzata (artt. 50 e ss. Codice consumo in tema di contratti a distanza in generale, nonchè discipline settoriali di contrattazione a distanza, come ad esempio quelle in materia di servizi finanziari ai consumatori, di cui all'art. 67 bis e ss. Codice consumo) attribuisce il diritto di recesso, e non in quelle in cui il destinatario del bene o del servizio sia un non consumatore, in quanto a tale soggetto il recesso può essere attribuito solo nelle ipotesi espressamente previste dal codice civile e non come disciplina di protezione, riequilibratice di un rapporto caratterizzato da connaturata asimmetria informativa.

In sintesi, sebbene ritengo che, alla luce dei risultati raggiunti dalla dottrina in questi anni, dei quali si è dato conto, non sia possibile affermare che l'invio di ricevuta dell'inoltro dell'ordine rappresenti una tappa del procedimento formativo del contratto a conclusione telematica, ugualmente un intervento di armonizzazione del legislatore comunitario, avente ad oggetto anche la determinazione dell'effettivo momento di conclusione del contratto, sarebbe stato senz'altro opportuno.

Anzi, proprio il fatto che in tre Stati, all'atto del recepimento di tale regola, sia stata avvertita l'opportunità di precisare come l'obbligo di accusare ricevuta dell'ordine interferisca con il comune procedimento di conclusione del contratto, conferma la sussistenza di dubbi al riguardo[55]. Si trattava però di questione che, attenendo alla armonizzazione della disciplina del

---

[54] Cfr. MANNA, La disciplina, cit., 136.

[55] In particolare, il Portogallo, ha previsto, nella legge di recepimento della direttiva sul commercio elettronico, che la conclusione dei contratti on line non segue lo schema comune, proprio in considerazione della circostanza che il procedimento formativo dell'accordo viene a completarsi soltanto con la conferma dell'ordine da parte del prestatore

contratto in generale, il legislatore comunitario non ha ritenuto di affrontare direttamente, preferendo inserire la previsione di un obbligo "generico", che non interferisse direttamente sulle singole discipline nazionali relative alla conclusione del contratto[56].

4. Responsabilità dell'hosting provider: problematiche attuali e prospettive

La questione della responsabilità civile degli isp è stata senz'altro una di quelle che più hanno interessato i giuristi a partire dal momento in cui internet ha cominciato a conoscere un uso commerciale e a divenire un mezzo di circolazione delle idee e della conoscenza a diffusione sempre più elevata, in grado di porsi come lo strumento di massima realizzazione della libertà di manifestazione del pensiero[57].

Non a caso, un profilo rilevante del dibattito sorto tra i civilisti in ordine alla necessità di introdurre nuove regole in conseguenza della diffusione delle tecnologie dell'informazione nello svolgimento dell'attività giuridica, cui facevo cenno nel primo paragrafo di questo scritto, ha riguardato l'esigenza o, quanto meno, l'opportunità di prevedere un coinvolgimento degli intermediari del commercio elettronico e della circolazione di contenuti in rete nella responsabilità per gli illeciti commessi via internet[58].

L'elevata potenzialità dannosa di tali illeciti, connessa alla natura aperta della rete ed alla sua diffusione policentrica delle conseguenze, unita alla non certo agevole identificabilità dell'au-

del servizio.

[56] Anche in considerazione del complesso percorso di definizione di principi europei in materia contrattuale (e non solo) in corso da anni ed il cui prodotto più recente è compiuto è rappresentato dal testo noto come Draft common frame reference, elaborato da un gruppo di giuristi europei ed avente ad oggetto la redazione di un complesso articolato, destinato a proporre una disciplina uniforme non solo per la materia contrattuale, ma anche dell'illecito e delle "altre" fonti delle obbligazioni.

[57] Per la descrizione delle varie di sviluppo dell'Internet, sono interessanti le pagine di un illustre epistemologo (FLORIDI, Internet, Milano, 1997); di recente, sempre dello stesso autore, può leggersi Infosfera: etica e filosofia dell'informazione, Torino, 2009.
Per le potenzialità di internet e per la sua capacità di porsi come il più formidabile strumento di realizzazione della libera manifestazione del pensiero, oltre che per una descrizione, tuttora attuale, della struttura acefala e decentrata della rete di reti, resta fondamentale la lettura della notissima decisione della Corte federale del Distretto orientale della Pennsylvania dell'11 giugno 1996 (leggibile su Dir. Inf., 1996, 604). In argomento si veda anche COSTANZO, Le nuove forme di comunicazione in rete: Internet, in Inf. e dir., 1997, 20.
La letteratura formatasi in questi ultimi anni in materia di r.c. degli internet service provider è vastissima. Mi limito a segnalare, senza alcuna pretesa di completezza, BUGIOLACCHI, (Dis)orientamenti giurisprudenziali in tema di responsabilità degli internet provider (ovvero del difficile rapporto tra assenza di obblighi di controllo e conoscenza dell'illecito, in Resp. Civ. prev., 2010, 1568; ID., La responsabilità dell'host provider alla luce del d.lgs. n. 70/2003: esegesi di una disciplina "dimezzata", in questa Rivista, 2005, 188; SANNA, Il regime di responsabilità dei providers intermediari di servizi della società dell'informazione, in questa Rivista, 2004, 279; D'ARRIGO, La responsabilità degli intermediari nella nuova disciplina del commercio elettronico, in Danno e resp., 2004, 249; PASQUINO, Servizi telematici e criteri di responsabilità, Milano, 2003; BOCCHINI, La responsabilità civile degli intermediari del commercio elettronico, Napoli, 2003; RICCIO, La responsabilità civile degli internet providers, Torino, 2002;.

[58] In argomento si veda, per un inquadramento generale della responsabilità civile nella società dell'informazione, si veda DI CIOMMO, Evoluzione tecnologica e regole di responsabilità civile, Napoli, 2003.

tore effettivo della condotta illecita, aveva fatto ipotizzare il possibile coinvolgimento degli isp, e soprattutto dei prestatori di hosting, in considerazione della loro attività di memorizzazione tendenzialmente duratura delle informazioni, la quale poteva far supporre una possibilità di controllo e/o di intervento sugli stessi[59]. Si ipotizzava cioè di imputare una responsabilità al provider, per fatto proprio ma a titolo concorrente (e soltanto eventuale) con l'effettivo autore della condotta illecita, anche nella prospettiva di evitare che i soggetti danneggiati restassero privi di risarcimento, vista la difficoltà di individuare l'effettivo autore dell'illecito, con evidente svilimento della funzione compensativa che ad oggi rappresenta l'elemento caratterizzante dell'istituto della responsabilità civile[60].

Come è noto, la reazione dei vari ordinamenti rispetto ad un tale, possibile coinvolgimento in presenza di illeciti perpetrati grazie alla nuova tecnologia, nella pressoché totale assenza di una normativa ad hoc, sia a livello sovranazionale che dei singoli stati, aveva generato un difficile lavoro della giurisprudenza, che però, in linea generale, aveva sempre evitato la canalizzazione della responsabilità verso i provider per gli illeciti commessi dai loro utenti sulla base della utilizzazione delle regole "speciali" di responsabilità presenti in vari ordinamenti civilistici europei[61].

Proprio la diversità degli approcci, consacrata nel considerando n. 40 della direttiva 2000/31 sul commercio elettronico, aveva indotto il legislatore comunitario a dettare regole armonizzate in tema di responsabilità di quei prestatori di servizi della società dell'informazione che svolgono un ruolo di intermediazione tecnica[62].

Senza voler qui ripercorrere il faticoso iter che, nel quadro della già di per sé complicata gestazione della direttiva, condusse alla costruzione della sezione quarta della direttiva 2000/31 (intitolata appunto"Responsabilità dei prestatori intermediari" e definita, in dottrina, una sorta di "legge nella legge"[63]), dedicata alla responsabilità degli isp, è sufficiente ricordare come la

---

[59] Sull'attività dell'host provider e sulle ragioni per le quali lo si è tradizionalmente ritenuto in grado di esercitare un controllo sulle informazioni memorizzate, si veda D'ARRIGO, La responsabilità degli intermediari nella nuova disciplina del commercio elettronico, in Danno resp., 2004, 249; BUGIOLACCHI, Verso un sistema della responsabilità civile dell'internet provider? Considerazioni su un recente "anteproyecto" spagnolo di recepimento della direttiva 2000731/CE sul commercio elettronico, in questa Rivista, 2002, 292.

[60] Per una interessante costruzione della responsabilità del provider quale ipotesi di illecito civile "plurisoggettivo permanente", si veda in dottrina BOCCHINI, La responsabilità civile degli intermediari del commercio elettronico, Napoli, 2003, spec. pagg. 203 e ss.

[61] Si pensi, ad esempio, all'ordinamento civilistico francese, il quale prevede, all'art. 1384 code civil, l'ipotesi di responsabilità del guardien, riconducibile, pur con le dovute differenze, alla responsabilità di cui all'art. 2051 c.c. italiano (sull'art. 1394 code civil francese può vedersi SICA, Circolazione stradale e responsabilità: l'esperienza francese e italiana, Napoli, 1980); oppure a quello spagnolo, nel quale, pur in assenza di una disposizione analoga, nel codigo civil, all'art. 2051 c.c., per la presenza di taluni articoli ce limitano solo ad alcune ipotesi specifiche il danno assimilabile a quello da cose in custodia di cui all'art. 2051 c.c., la giurisprudenza ha comunque consentito di fornire una tutela rafforzata, soprattutto mediante l'inversione dell'onere della prova, anche al danneggiato da attività e da cose non espressamente previste nel testo codicistico. In tema di costruzione giurisprudenziale della figura generale del danno da cose nell'ordinamento spagnolo, si veda in dottrina MEZZASOMA, Il danno da cose negli ordinamenti italiano e spagnolo, Napoli, 2001.

[62] Afferma il considerando n. 40 che la ragione di apprestare regole di responsabilità dei "prestatori intermediari" sono necessitate dalle divergenze tra le legislazioni e le impostazioni giurisprudenziali degli stati membri, tali, appunto, da produrre effetti discorsivi della concorrenza nel mercato interno.

[63] Così COMANDE' e SICA, Il commercio elettronico. Profili giuridici, Milano, 2001, 228.

scelta europea fu ispirata alla scelta di evitare di esporre tali soggetti a responsabilità eccessivamente gravose (come quelle derivanti dall'imputazione di responsabilità mediante criteri oggettivi o semi-oggettivi), al fine di non disincentivarne l'attività proprio nella fase di avvio del commercio elettronico, optando per un netto recupero dell'elemento soggettivo della colpa. Ciò non nel senso tradizionale di scostamento da non meglio specificati canoni di diligenza, prudenza e perizia, il cui accertamento si presta comunque a valutazioni discrezionali, bensì attraverso l'utilizzazione della colpa "tipizzata" o "specifica", legata a condotte ugualmente tipizzate rispetto alle quali il legislatore ha operato una valutazione predeterminata, idonea ad evitare al giudice di dover stabilire, caso per caso, se vi sia stato, nella condotta del provider, lo scostamento da uno standard di diligenza da lui esigibile [64].

Nel sistema delineato di responsabilità del provider disegnato dalla direttiva il fulcro era (ed è) rappresentato dal principio dell'assenza di un obbligo generale di "sorveglianza" del provider sulle informazioni ospitate, come pure dell'obbligo di svolgere una ricerca attiva di materiali illeciti sui siti gestiti [65].

Come pure è noto, in relazione ai presupposti della responsabilità dell'host provider, l'art. 14 della direttiva ha individuato due condizioni, chiaramente debitrici della impostazione contenuta nel DMCA (Digital Millenium Copyright Act) statunitense del 1998: la conoscenza della illiceità dell'attività o dell'informazione e l'omessa rimozione della attività o della informazione[66].

Dopo l'emanazione della direttiva, l'interesse dei commentatori per il nuovo regime è stato alimentato soprattutto da due profili: 1) intanto, il fatto che fosse stato creato un nuovo regime speciale di responsabilità, il che rappresentava anche un laboratorio di verifica delle tendenze in atto nella costruzione di un possibile diritto europeo della responsabilità civile[67]; 2) la critica avente ad oggetto la genericità di taluni aspetti decisivi della disciplina, tali da mettere fortemente a rischio la realizzazione di una effettiva armonizzazione all'atto del recepimento da parte degli stati membri, con particolare riferimento alla eccessiva vaghezza della nozione di manifesta illiceità dell'informazione o dell'attività e, soprattutto, di quella di conoscenza dei fatti o delle attività illecite, di rilevanza assolutamente centrale, in quanto costituente il presupposto necessario dell'intervento di rimozione da parte dell'host provider, cui si univa anche quella della mancata previsione delle modalità di rimozione dei contenuti (il c.d. procedimento

---

[64] Sul complesso e tortuoso iter che condusse alla formulazione definitiva del regime di responsabilità degli isp di veda BOCCHINI, La responsabilità civile degli intermediari, cit., spec. 109 e ss.
Sulle caratteristiche del regime di responsabilità degli isp, incentrato appunto su ipotesi di colpa legislativamente tipizzate, si veda, per tutti, BUGIOLACCHI, La responsabilità dell'host provider, cit., 193; PONZANELLI, Verso un diritto uniforme per la responsabilità dell'Internet provider, cit., 8.

[65] Termine utilizzato nella direttiva e poi trasposto pedissequamente dalla nostra legislazione di recepimento, sebbene ignoto alla nostra legislazione civilistica. Sulla ratio e le conseguenze dell'introduzione di tale principio, si veda in dottrina PINO, Assenza di un obbligo generale di sorveglianza a carico degli Internet service providers sui contenuti immessi da terzi in rete, in Danno resp., 2004, 834; RICCIO, La responsabilità degli internet providers nel d.lgs. n. 70/2003, ivi, 2003, 1158; sia anche consentito il rinvio a BUGIOLACCHI, La responsabilità dell'host provider, cit., 192.

[66] Sul fatto che la responsabilità del provider di hosting trovi il suo "criterio di collegamento" nella ricorrenza congiunta della citate condizioni, concorda la maggior parte della dottrina italiana (PASQUINO, Servizi telematici e criteri di responsabilità, cit., 292; PONZANELLI, Verso un diritto uniforme, cit., 7; BOCCHINI, La responsabilità civile degli intermediari, cit., 153.

[67] In argomento si veda SICA, Note in tema di sistema e funzione della regola aquiliana, in Danno resp., 200, spec. 196.

di notice and take down, che va dalla conoscenza alla rimozione, disciplinato ad esempio dal DMCA)[68]. Conseguentemente, non è risultato affatto chiaro se per conoscenza dell'illecito da parte del provider dovesse intendersi anche la mera segnalazione proveniente da qualunque soggetto (anche lo stesso danneggiato) o se fosse necessaria la provenienza della stessa da una fonte "qualificata", come l'autorità giudiziaria o un'autorità amministrativa competente sull'illecito.

Una siffatta indeterminatezza ha fatto sì che all'atto del recepimento, taluni stati membri abbiano avvertito l'esigenza di specificare la nozione di conoscenza dell'illecito: è quanto ha fatto il legislatore italiano, con il primo comma, lett. b) dell'art. 16 del d.lgs. n. 70 del 2003, prevedendo che l'host provider sia responsabile una volta che, avuta conoscenza del materiale illecito "su comunicazione delle autorità competenti", non provveda a rimuoverlo[69].

Ne è risultata una disciplina non armonizzata, visto che in altri stati membri non è stato richiesto il carattere qualificato della conoscenza quale presupposto dell'obbligo di rimozione dei contenuti da parte del provider[70].

La questione è stata ulteriormente complicata dal fatto che la giurisprudenza italiana successiva al recepimento della direttiva 2000/31[71], contrariamente all'orientamento dottrinario prevalente[72], ritiene che condizione necessaria e sufficiente per l'attribuzione di responsabilità nei confronti dell'host provider che non abbia rimosso i contenuti illeciti, sia rappresentata dalla mera conoscenza dell'illiceità da parte sua, la quale può derivare da acquisizione autonoma o da segnalazione da parte di qualsivoglia terzo.

La divergenza di posizioni interpretative sul punto non ha però provocato un grande dibattito presso gli operatori del diritto, probabilmente anche in considerazione dell'esiguo numero di casi giurisprudenziali aventi ad oggetto la responsabilità del provider per illeciti commessi mediante internet, collegata anche ad un più generale diminuito interesse alla questione da parte dell'opinione pubblica, con la conseguenza che essa è stata affrontata forse più spesso da una prospettiva comparatistica, con riferimento a casi giurisprudenziali emersi in altri paesi, con maggior frequenza che nel nostro.

Col senno di poi, possiamo ora dire che si trattava solo di questione di tempo, dato che nell'ul-

---

[68] Per tali critiche si veda in dottrina RICCIO, La responsabilità, cit., 205.
Sulla individuazione della conoscenza dell'illecito e della successiva inerzia, quali condizioni necessarie per l'attribuzione di responsabilità al provider, sulla scia di quanto stabilito dal legislatore statunitense (anche se limitatamente al diritto d'autore) con il Digital Millenium Copyright Act, sussiste accordo press o la nostra dottrina. Si veda, per tutti, BOCCHINI, La responsabilità civile degli intermediari, cit., 153; COMANDE' e SICA, Il commercio elettronico. Profili giuridici, cit., 229; DI CIOMMO, Evoluzione tecnologica e responsabilità civile, cit., 293.

[69] Analoga precisazione, rispetto al testo della direttiva, si trova nella legge spagnola di recepimento (Ley n. 34 del 2002).

[70] Ad esempio in Francia (legge n. 575 del 2004) ed in Portogallo (decreto ley n. 7 del 2004). Anche se in quest'ultimo paese l'art. 18 del citato decreto consente a qualsiasi terzo di rivolgersi ad una autorità tenuta, per legge, ad effettuare una valutazione provvisoria sulla illiceità del materiale, entro 48 ore dalla richiesta, al cui esito il provider è tenuto ad adeguarsi.

[71] In questo senso Trib. Catania, 29 giugno 2004, in Responsabilità civile e previdenza, 2005, 188; Trib. Bari, 13 giugno 2006, in Diritto dell'internet, 2006, 563; Trib. Trani, 14 ottobre 2008, in Danno e responsabilità, 2008, 1050.

timo anno una serie di pronunce giurisprudenziali, tutte peraltro accompagnati da una dirompente eco mediatica, hanno portato nuovamente alla ribalta, come senz'altro mai era accaduto prima, la tematica delle responsabilità in rete e quella, intimamente connessa, del ruolo degli isp rispetto ai contenuti immessi in rete dagli utenti dei loro servizi.

Il riferimento è alla nota vicenda che ha visto sottoposti a procedimento penale i vertici di Google Italia, in quanto imputati di concorso in diffamazione, con l'uploader del materiale lesivo che aveva caricato sulla piattaforma digitale "Google Video", un filmato palesemente offensivo dell'onore, della reputazione e della dignità di un adolescente affetto da sindrome di Down; a quella, altrettanto nota, relativa alla richiesta di rimozione delle riproduzioni di "spezzoni" della trasmissione "Grande Fratello 10", effettuata dai titolari dei relativi diritti di autore nei confronti di Youtube, piattaforma di contenuti, anch'essa di proprietà di Google, sulla quale detti spezzoni, immessi dagli utenti, erano memorizzati e resi accessibili a qualunque terzo.

La concomitanza temporale delle due vicende non rappresenta probabilmente un caso, in quanto, come è stato rilevato in dottrina, l'uso ormai generalizzato dei motori di ricerca, dei social network e delle piattaforme digitali di condivisione di contenuti ad accesso libero e alimentate dall'attività di uploading degli stessi utenti/fruitori (servizi cc.dd. di ugc: user generated content) hanno amplificato a dismisura la facilità di immissione di contenuti (anche illeciti) e reso più agevole la loro reperibilità e percezione da parte dei soggetti danneggiati e dei terzi in genere, ben oltre la popolarità dello spazio web ove i contenuti erano stati (eventualmente) originariamente collocati[73]. Al tempo stesso, proprio la grande diffusione presso il pubblico di queste piattaforme, che configurano un servizio di hosting, ha concretizzato quel timore di elevata potenzialità dannosa degli illeciti commessi via internet di cui si discorreva anni fa, ma che sembrava essere stato smentito nei fatti.

Non essendo questa la sede per effettuare una disamina approfondita delle due pronunce cui si è appena fatto cenno, ci si limiterà a evidenziare come in entrambe si avverta il tentativo di pervenire alla esatta individuazione delle condizioni di responsabilità degli isp per i contenuti illeciti che essi, pur non essendone autori, veicolano sulla rete, alla quale si lega strettamente quella della individuazione della portata da attribuire al principio generale dell'assenza dell'obbligo di sorveglianza sul materiale.

Si tratta probabilmente di una conseguenza del fatto che il regime speciale di responsabilità degli isp disegnato dalla direttiva, come già accennato, non è mai stato sufficientemente chiaro,

---

[73] Sul punto sia consentito il rinvio a BUGIOLACCHI, (Dis)orientamenti, cit., spec. 1573 e ss. Ciò è evidente per quanto riguarda i motori di ricerca, la cui attività di indicizzazione aumenta enormemente la visibilità di contenuti immessi inizialmente in rete su siti magari non dotati di particolare diffusione e notorietà presso il pubblico degli utenti della rete. Sulle problematiche giuridiche connesse ai servizi forniti dai motori di ricerca, si veda in dottrina COSTANZO, Motori di ricerca: un altro campo di sfida tra logiche del mercato e tutele dei diritti?, in Dir. Internet. 2006, 545: SAMMARCO, Il motore di ricerca, nuovo bene della società dell'informazione: funzionamento, responsabilità e tutela della persona, in Dir. Inf., 2006, 4.
Giova ricordare come il legislatore comunitario abbia deciso, in sede di redazione della direttiva 2000/31, di rinviare ai successivi adeguamenti della disciplina, la questione del regime di responsabilità dei motori di ricerca (i quali, da un punto di vista tecnico, effettuano attività di caching, anche se tendente a trasformarsi, stante il carattere duraturo della indicizzazione o anche della stessa copia cache in attività di memorizzazione permanente dei contenuti, assimilabile piuttosto a quella degli host provider).

soprattutto per quanto attiene alla determinazione dei presupposti per l'attivazione, da parte del provider di hosting, della procedura di rimozione delle informazioni illecitamente caricate in rete; da questo punto di vista, poi, la normativa italiana di recepimento, ha finito in un certo senso per acuire le criticità originarie, in quanto, pur avendo delimitato la nozione di conoscenza dell'illecito da parte del provider, dalla quale soltanto, come noto, scaturisce l'obbligo di rimozione/disabilitazione dei contenuti, ad una conoscenza "qualificata", consistente cioè nella "comunicazione" dell'illecito che il provider riceva da parte delle autorità competenti (così l'art. 16, secondo comma, lett. b, d .lgs. n. 70 del 2003), non ha affatto specificato (né demandato ad una disciplina di dettaglio) il procedimento all'esito del quale la non meglio precisata autorità competente provveda ad informare l'host provider né la tempistica che dovrebbe caratterizzare l'intera procedura di notice and take down, con la conseguenza che chi scrive non ha esitato a definire "dimezzata" la disciplina di recepimento in tema di responsabilità da attività di hosting[74].

Ne è risultata una accentuazione della tendenza, già presente soprattutto da parte dei colossi dell'hosting quali Google, a non attivarsi in presenza di segnalazioni, anche numerose, ed anche se relative a contenuti palesemente illeciti, non potendosi inferire, alla luce della normativa italiana vigente, dalle semplici segnalazioni provenienti da terzi (compresi i pretesi danneggiati) quella condizione di conoscenza "qualificata" richiesta dalla norma italiana di recepimento.

L'appena citato tentativo da parte della giurisprudenza di fissare regole più chiare, che rendessero maggiormente "operativa" la disciplina sulla responsabilità degli host provider, è stato perseguito praticando percorsi argomentativi non uniformi, ma caratterizzato da profili di univocità, come si vedrà confrontando i casi che, per semplicità, potremmo denominare "Google" e " Youtube".

Si assiste, infatti, da un lato al ricorso a strumenti di tutela attinti da altre fonti normative rispetto a quelle che configurano il regime di r.c. dei provider (il riferimento è all'utilizzazione della disciplina sulla protezione dei dati personali per imputare una responsabilità ai vertici di google italia, a fronte della riaffermazione della regola dell'assenza di un obbligo di sorveglianza prevista dalla direttiva comunitaria 2000/31 e dal decreto italiano di recepimento); dall'altro, viene dapprima riconfermata la centralità del principio dell'assenza di un obbligo di sorveglianza preventiva, ma poi si pretende dal gestore della piattaforma di contenuti di attivarsi per evitare la reiterazione futura di violazione di altrui diritti su opere dell'ingegno, con implicita attribuzione di un obbligo di monitoraggio e controllo sui contenuti veicolati che, oltre che contraddittorio, pare anche porsi in contrasto con il citato principio cardine della assoluta assenza di un obbligo di controllo.

In entrambi i casi, a prescindere dal decisum, viene assegnato particolare rilievo agli interventi effettuati dal provider sui materiali caricati dai terzi (indicizzazione, categorizzazione, classificazione, ma anche di previsione di politiche di gestione "autonoma" dei contenuti ospitati, concretantesi nella sospensione unilaterale del servizio, nella facoltà di rimozione di contenuti, etc.) che, anche e soprattutto in quanto funzionali a fargli ottenere un cospicuo ritorno economico, gli farebbero eccedere il ruolo di intermediario meramente tecnico, rendendolo

[74] Per tali valutazioni sia consentito il rinvio a BUGIOLACCHI, La responsabilità dell'host provider, cit.,206.

responsabile per i contenuti oggetto di uploading, come pure l'insensibilità dell'intermediario alle diffide provenienti dai soggetti ritenutisi danneggiati. Si assiste quindi ad una valorizzazione della condotta concretamente tenuta dal provider rispetto ai contenuti, vale a dire un elemento che non è stato assolutamente preso in considerazione dal legislatore comunitario se non per il caso in cui l'intermediario rivestisse anche il ruolo di content provider (cioè non solo intermediario tecnico ma anche fornitore-creatore del materiale immesso on line).

In questo modo viene anche ad essere indirettamente avallato l'orientamento, già descritto, della giurisprudenza italiana successiva al recepimento della direttiva 2000/31, la quale ritiene condizione necessaria, ma sufficiente, per la attribuzione di responsabilità in capo al provider, la conoscenza, da parte sua, dell'attività o dell'informazioni illecita, tratta semplicemente dalla segnalazione proveniente da qualunque terzo o dalla valutazione autonoma di una manifesta illiceità, e pertanto in palese contrasto con quanto risultante dalla opzione del legislatore del recepimento per una nozione di conoscenza come conoscenza "qualificata"[75].

Si tratta di un profilo che non riguarda soltanto l'interpretazione delle regole di r.c. in in materia ed il loro coordinamento con le regole riguardanti altri ambiti di tutela (come quelli della protezione dei dati personali e delle opere delle ingegno on line) ma, come quasi sempre accade quando le attività giuridiche incidono su aree ad elevata rilevanza economico-sociale, diviene questione di politica del diritto, in quanto in grado di influenzare (incentivandoli o disincentivandoli) i modelli commerciali innovativi che le nuove piattaforme di hosting rendono possibile, costringendo così l'operatore del diritto ad interrogarsi sulla persistente attualità delle regole dettate in materia dal legislatore comunitario nell'ormai lontanissimo anno 2000.

Volendo ripercorrere, con rapida sintesi, i percorsi argomentativi seguiti dai giudici nei casi "Google" e "Youtube", possiamo osservare che, nel primo, i magistrati inquirenti ipotizzavano in capo ai vertici aziendali di Google Italia una responsabilità per omessa rimozione del video postato sulla piattaforma di sharing " Google video", nel quale un soggetto disabile veniva chiaramente diffamato; tale responsabilità veniva fatta derivare dalla considerazione che il provider non poteva ignorare l'esistenza di un video che risultava tra i più cliccati (tanto da essere collocato ai primi posti nelle classifiche) oltre che da quella secondo cui Google non si limitava ad un ruolo meramente tecnico, di memorizzazione dei contenuti caricati dagli utenti, ma assumeva un ruolo attivo su di essi, tipico di un provider "attivo", consistente nella loro categorizzazione, finalizzata, per giunta, al proprio profitto, derivante dal miglior abbinamento tra contenuti presenti in piattaforma e annunci e/o link pubblicitari, secondo il business model noto come AD Words.

Il Tribunale di Milano, però, con la sentenza emessa il 12 aprile 2010, pur auspicando un intervento del legislatore che rende il provider, nei fatti, più facilmente responsabile per omesso controllo, sulla base della considerazione che il progresso tecnico consentirebbe ormai di controllare in modo sempre più stringente il caricamento dei dati e di predisporre idonei filtri preventivi, ha disatteso l'impostazione degli inquirenti, ritenendo condivisibilmente che, alla luce della normativa vigente (in particolare, art. 17 d.lgs. n. 70 del 2003, che recepisce il principio europeo sull'assenza di obblighi di sorveglianza), non esista un obbligo di legge che

[75] Si veda ad esempio in tal senso, in giurisprudenza, Trib. Catania, in Resp. Civ. prev., 2005, 188.

imponga al provider un controllo preventivo sulla innumerevole serie di dati memorizzati che "passano ogni secondo nelle maglie dei gestori dei siti web", ed ha quindi respinto gli addebiti di concorso del provider nel reato di diffamazione. Ne è invece derivata, come è noto, la condanna di taluni esponenti dei vertici aziendali di Google Italia, fondata però sulla normativa in tema di protezione dei dati personali (d.lgs n. 196 del 2003), la quale imporrebbe agli hosting provider – e quindi a Google – nell'esercizio del dovere di "corretta informazione" di invitare i propri utenti a verificare che l'uploading avvenga nel rispetto del diritto alla protezione dei dati personali dei terzi.

Il caso Youtube è emblematico della sempre maggior rilevanza della problematica della legittimità dell'uploading di opere protette (o anche di semplici "spezzoni" di queste) sulle grandi piattaforme ugc, alla quale è strettamente connessa quella relativa alla responsabilità degli host provider che forniscono lo spazio ove tali contenuti vengono caricati.

La pronuncia trae spunto dalla causa promossa dal gruppo RTI (Mediaset) nei confronti di Youtube al fine di ottenere da quest'ultimo un maxirisarcimento per essersi reso responsabile, o almeno corresponsabile, per le violazioni in materia di copyright commesse, in via diretta, dagli uploaders di materiali protetti. Nell'ambito di questo procedimento, Rti ha richiesto in via cautelare la rimozione immediata di tutti i frammenti della produzione televisiva "grande fratello 10", ottenendola con una prima ordinanza del dicembre 2009, il cui contenuto è stato ribadito da una seconda, dell'11 febbraio 2010, emessa in seguito al reclamo proposto da Youtube[76].

Le due ordinanze sono caratterizzate da una serie di argomentazioni che meritano di essere riprodotte.

A)In primo luogo il tribunale romano, pur non decidendo sulla questione della responsabilità del provider, rimandata alla sentenza che definirà il giudizio nel merito, ha affermato che, sebbene non sussista un obbligo del provider di sorvegliare i contenuti, questi non possa essere esonerato da responsabilità nel caso in cui ecceda un ruolo meramente tecnico, intervenendo sui contenuti, anche al solo fine di renderli individuabili dagli utenti e soprattutto quando, pur essendo consapevole della presenza di materiale sospetto, si astenga dall'accertarne la illiceità e dal rimuoverlo, con una interpretazione non condivisibile alla luce della previsione normativa la quale, come detto, condiziona l'obbligo di intervento del provider alla conoscenza "qualificata" dell'illiceità.

Nel passaggio motivazionale forse più rilevante, viene specificato come il fornitore di hosting non possa essere considerato irresponsabile per il solo fatto che la gestione dei contenuti sulle piattaforme ugc sia soltanto di chi li ha caricati, non potendosi ipotizzare un obbligo del provider di controllarli e di disabilitarne l'accesso ove ritenuti illeciti e viene poi aggiunto come, in accordo con la giurisprudenza più recente, si debba attribuire rilevanza alle attività (o omissioni) dell'intermediario: se infatti è vero, secondo tale impostazione, che in tale materia viga il principio dell'assenza di un obbligo generale di sorveglianza sui contenuti, ciononostante il provider non potrebbe andare esente da responsabilità ove predisponga un

[76] La prima, del 16 dicembre 2009, può leggersi in Responsabilità civile e previdenza on line, all'indirizzo web www.giuffre.it/riviste/resp.

controllo delle informazione e, soprattutto, quando, pur essendo consapevole della presenza di materiale sospetto, si astenga dall'accertarne la illiceità e dal rimuoverlo. Nel caso di specie, Nel caso di specie, secondo il tribunale, il provider si sarebbe responsabile, in proprio ed in via concorrente con l'uploader di contenuti protetti, per: a) aver organizzato la gestione dei contenuti video caricati sulla piattaforma, anche programmandone e disciplinandone la visione (in considerazione del fatto che sulla piattaforma è anche possibile scegliere le singole parti di trasmissione – un giorno, un episodio specifico – cui si intende accedere), e ciò anche al fine di ottenere un ritorno commerciale; b) l'essere rimasto insensibile alle ripetute diffide inviate da Rti, pur nella consapevolezza della spettanza dei diritti in via esclusiva, su quei contenuti, alla stessa Rti; c) il fatto di avere, in concreto, adottato delle "regole" relative all'immissione e gestione dei contenuti da parte degli utenti, dalle quali si evincerebbe la volontà/possibilità di esercitare un controllo sulle informazioni veicolate[77].

L'insieme di tali comportamenti sarebbe, ad avviso del tribunale, inconciliabile con la addotta mera "messa a disposizione della piattaforma".

Come ho accennato poco sopra, è innegabile, come peraltro afferma lo stesso giudice, che la giurisprudenza italiana, successiva al recepimento della direttiva sul commercio elettronico, abbia dato, delle regole sulla responsabilità dell'hosting provider, una lettura simile a quella effettuata nella ordinanza in commento. Secondo una tale lettura della normativa vigente, effettuata ad esempio dal Tribunale di Catania, sarebbe sufficiente una qualunque segnalazione della presunta illiceità di una attività o di una informazione, a prescindere dalla natura (il preteso danneggiato, un qualunque terzo, una autorità competente) del soggetto dal quale la segnalazione provenga; a quel punto la provenienza della segnalazione da una autorità competente (che secondo la lettera e l'interpretazione del sistema risultante dagli artt. 16 e 17 d.lgs. 70/2003 e la sola a legittimare il provider alla rimozione del contenuto, come si è già accennato) avrebbe il solo effetto di fra transitare la fattispecie da una ipotesi di responsabilità colposa ad una dolosa.

Anche la cassazione penale, in una recente pronuncia, analogamente a quanto effettuato dal tribunale di Roma, nel valutare la sussistenza di un concorso dell'host provider nel reato commesso dall'utente, ha ricostruito il sistema di cui agli artt. 16 e 17 d.lgs. n.70 del 2003, nel senso che laddove il fornitore di hosting non si limiti a mettere a disposizione degli utenti la piattaforma di sharing, ma a ciò accompagni una attività ulteriore, quale quella di "indicizzazione" delle informazioni provenienti dagli utenti/generatori di contenuti, cessa di svolgere una attività meramente intermediativa, incorrendo in responsabilità, con interpretazione tranquillamente trasferibile in ambito civilistico[78].

Una tale impostazione non mi pare però condivisibile, avuto riguardo all'art. 16 del d.lgs. 70/2003, dedicato appunto alla responsabilità dell'host provider. Tale disposizione mantiene la medesima tecnica di redazione legislativa del suo omologo comunitario (art. 14 direttiva), strutturando le circostanze di cui al comma 1, lettere a) e b), come condizioni di esenzione

---

[77] A questo specifico riguardo il tribunale elenca alcune di tali "regole".

[78] Si tratta di Cass. Pen., 23 dicembre 2009, n. 49437, inedita, resa nel noto caso che aveva visto coinvolto la piattaforma di file sharing Pirate Bay.

da responsabilità. Se però la lettera a), nella sua seconda parte, quella attinente alla r.c., ricalca pedissequamente l'art. 14 della direttiva, la lettera b) presenta una rilevantissima novità, in quanto, diversamente dalla direttiva (art. 14, comma 1, lett. b) e dalla stessa legge delega (legge 39 del 2002), introducendo l'inciso "su comunicazione delle autorità competenti", prende espressamente ed inequivocabilmente posizione sulla necessità di una "ufficializzazione" della conoscenza attraverso la sua formalizzazione da parte di autorità pubbliche[79].

In questo modo il legislatore italiano, probabilmente allo scopo di ridurre l'area di indeterminatezza della nozione di "conoscenza" da parte del provider risultante dalla direttiva, ha prodotto (sarebbe più corretto dire avrebbe dovuto produrre, stante il citato orientamento giurisprudenziale prevalente) un restringimento della responsabilità del provider di hosting, non più tenuto ad effettuare valutazioni inesigibili da un punto di vista della competenza professionale e dal punto di vista strettamente tecnico (vista la mole immensa di contenuti continuamente caricati sulle grandi piattaforme ugc) in ordine alla configurabilità o meno dell'illiceità del materiale segnalatogli, in quanto potrà (e dovrà) procedere alla rimozione soltanto quando la notice della illiceità gli pervenga dalle citate autorità competenti[80].

La soluzione prospettata dal tribunale di Roma, oltre che dalla giurisprudenza successiva al recepimento della direttiva potrebbe giustificarsi soltanto ove si riconoscesse una autonoma portata precettiva alla lettera a) del primo comma dell'art. 16 d.lgs. 17 del 2003, ovverosia facendo dire a tale "frammento" normativo, il quale assume significato precettivo solo ove letto unitamente alla lettera b) dello stesso comma, quello che in realtà non dice, e cioè che il provider sia responsabile ogni volta che, al corrente della manifesta illiceità del contenuto, su segnalazione di chicchessia, non si sia attivato per rimuoverlo[81].

Ne risulta, ad avviso di chi scrive, che alla luce della disciplina vigente nel nostro paese, l'hosting provider non sia abilitato a compiere alcuna attività di rimozione di contenuti illeciti, anche laddove il loro carattere antigiuridico sia manifesto, in assenza di una comunicazione delle autorità competenti, il che non toglie che la nozione di conoscenza "qualificata" cui il nostro legislatore condiziona l'intervento del provider, in assenza della definizione di una procedimentalizzazione del sistema (in che modo le autorità competenti ottengono l'infor-

---

79 Così, in dottrina, BUGIOLACCHI, La responsabilità dell'host provider, cit., 198; nello stesso senso COMANDE', Al via l'attuazione della direttiva sul commercio elettronico, ma … serve un maggior coordinamento, cit., 812; RICCIO, La responsabilità degli internet provider nel d.lgs. n. 70/2003, cit., 1162. Di recente, nel medesimo senso, CASAROSA, Wikipedia: esonero dalla responsabilità, in Danno e resp., 2009, 149; TRUCCO, Pubblicazione d'immagini personali in rete e responsabilità del provider, n Dir. Internet, 2006, 565; MANNA, La disciplina del commercio elettronico, Padova, 2005, 205 MANNA, La disciplina del commercio elettronico, cit., 205 e s., la quale evidenzia come il legislatore italiano abbia opportunamente evitato, in questo modo, di addossare al provider l'obbligo di rimozione su segnalazione di provenienza non autoritativa, eliminando anche il rischio connesso alla rimozione indebita.

80 In questo senso sia consentito il rinvio a BUGIOLACCHI, La responsabilità dell'host provider, loc. ult. Cit., TRUCCO, Pubblicazione d'immagini personali in rete, cit., 565; BOCCHINI, La responsabilità civile degli intermediari, cit., 156.

81 E' questa l'impostazione, ad oggi invero isolata in dottrina, di CASSANO e CIMINO, Il nuovo regime di responsabilità dei providers: verso la creazione di un novello "censore telematico", in Corr. Giur., 2004, 91. secondo i quali, ove la responsabilità del provider di hosting fosse disciplinata dalla lettera b) (con obbligo di rimozione scaturente solo a seguito di comunicazione delle autorità competenti), si perverrebbe ad una interpretazione abrogante della lettera a); ma così non è, come sinteticamente motivato supra, nel testo.

mazione relativa ad una presunta illiceità dei contenuti? entro quanto ne informano l'host provider e con quali modalità?, tanto per citare qualcuno dei profili problematici) finisca per rendere scarsamente efficiente la disciplina di notice and take down risultante dal d.lgs. n. 70 del 2003[82].

B)Se quello appena descritto è il profilo senz'altro più rilevante dell'ordinanza, ve n'è un altro che pure merita di essere affrontato.

Esso attiene al contenuto dell'ordine emesso dal tribunale di Roma in accoglimento del ricorso presentato da Rti. Il giudice capitolino, infatti, oltre ad aver ordinato alle resistenti l'immediata rimozione dai propri server e la conseguente disabilitazione di tutti i contenuti riproducesti sequenze di immagini fisse o in movimento relative al programma "Grande Fratello" decima edizione, inibisce loro il proseguimento della violazione dei diritti connessi di utilizzazione e sfruttamento economico del programma in questione.

Il contenuto di tale ultima inibitoria suscita infatti più di una perplessità, in quanto fa ritenere che il giudice intenda obbligare il provider all'adozione di una serie di provvedimenti finalizzati ad evitare la ripetizione, nel futuro, di ulteriori violazioni dello stesso segno di quelle così inibite[83].

E' innegabile che un ordine siffatto, per essere adempiuto, dovrebbe prevedere lo svolgimento, da parte del provider, di una continua attività di monitoraggio del materiale postato, operazione pressoché impossibile tecnicamente, oltre che contrastante con il più volte citato principio fondamentale dell'assenza di un obbligo di sorveglianza, il quale si esplicita, secondo il dettato europeo (art. 15 direttiva 2000/31) ed italiano (art. 17 d.lgs. n. 70 del 2003), proprio nel mancato assoggettamento dei provider sia ad un obbligo generale di sorveglianza sulle informazioni che trasmettono o memorizzano che ad uno di ricerca attiva di fatti e circostanze che indichino la presenza di attività illecite.

Non sembra neppure sostenibile che un tale obbligo di sorveglianza, implicito nella inibitoria "pro futuro", possa trarre il suo fondamento nel carattere speciale di talune disposizioni di legge, quali gli artt. 156 e 163 della lda, o in ragione della particolare natura dei diritti lesi.

Infatti, quanto ad un preteso carattere "speciale" della contenuta negli artt. 156 e 163 lda, deve essere rilevato come entrambi siano stati modificati a seguito dell'entrata in vigore del d.lgs. n. 140 del 2006, con il quale è stata recepita nel nostro ordinamento la direttiva 2004/48/CE (c.d. direttiva enforcement), finalizzata a rafforzare la protezione dei diritti di proprietà intellettuale. Un chiaro esempio della finalità di adattamento della nuova normativa anche alle possibilità tecnologiche offerte dalla rete, è rappresentata proprio dall'art. 156 lda, invocato dai ricorrenti, dato che tale disposizione, nella formulazione introdotta appunto con il d.lgs. n. 140 del 2006, prevede che il provvedimento inibitorio possa essere richiesto non solo nei confronti dell'autore della violazione, ma anche contro l'intermediario (il provider di hosting

[82] E' per questo che chi scrive ha qualificato come "dimezzata" la disciplina relativa alla responsabilità del provider di hosting.

[83] Non sembrano esservi dubbi su tale interpretazione dell'inibitoria, anche in considerazione di quanto ritenuto dal giudice, in un frammento della parte motiva, ove compie riferimento alla situazione in cui si troverebbe la ricorrente ove dovesse intentare un giudizio per ogni continua violazione dei propri diritti di utilizzazione economica.

o, eventualmente, di caching), i cui servizi siano stati utilizzati per commettere l'illecito. Nel far ciò, però, il secondo comma del così modificato art. 156 lda, "fa salve le disposizioni di cui al d.lgs. n. 70 del 2003".

Questa clausola di salvezza non può che essere interpretata nel senso che, una cosa è la "direzione" del provvedimento inibitorio, che può avere come destinatario anche il provider, altra cosa è la valutazione della condotta di quest'ultimo, la quale non può che essere effettuata secondo le regole del sistema di responsabilità speciale dell'isp contenuto appunto nel d.lgs. 70/2003[84].

La conseguenza è che, anche di fronte ad una violazione del diritto d'autore, commessa grazie alla intermediazione di un provider di hosting, quest'ultimo non potrà mai essere considerato responsabile se non al di fuori dei casi espressamente previsti dal regime di cui al citato decreto 70/2003 né potrà essere assoggettato ad un obbligo di sorveglianza non previsto da tale ultimo decreto[85]..

Sembra quindi di assistere, nella giurisprudenza italiana, ad incertezze nella interpretazione della normativa europea e di quella interna di recepimento, talvolta tali da stravolgere lo spirito della direttiva 31/2000: è infatti evidente che la sottoposizione del provider ad un obbligo preventivo di verifica della titolarità dei diritti di utilizzazione economica da parte degli uploaders, oltre che impositiva di obblighi di valutazione non esigibili, sarebbe caratterizzata dal rischio di indurre meccanismi di overdeterrence nei confronti dei provider i quali, timorosi di vedersi addossare responsabilità, potrebbero eccedere nel limitare "a monte" il caricamento di contenuti, con evidente compressione della circolazione delle idee.

Quanto detto non significa che le regole in tema di responsabilità dei provider per i contenuti veicolati non siano migliorabili, tanto è vero che chi scrive le ha già in altra sede criticate[86], sia per l'indeterminatezza della disciplina europea che per i difetti della normativa italiana di recepimento la quale, nell'introdurre la nozione di conoscenza qualificata, non specifica quali siano le "autorità competenti" deputate a dialogare con l'host provider né quali siano modalità e tempistica della procedura di comunicazione e rimozione dei contenuti illeciti.

Incertezze interpretative analoghe, originate anche dalla difficoltà di rispondere alla pressione sociale esercitata dalle richieste dei danneggiate in presenza di una normativa non chiara (e quindi non efficiente) si riscontrano anche presso altri stati membri, se solo si pensa che nel settembre 2010 il Tribunale commerciale di Madrid, nel decidere sull'appello proposto da Youtube nei confronti di Telecinco in una vertenza pressoché identica a quella qui descritta,

---

[84] In argomento si veda in dottrina SAVORANI, Diritto d'autore: rimedi civilistici dopo la direttiva enforcement, in Danno resp., 2007, 500.

[85] Una tale interpretazione ci pare l'unica possibile, sia alla luce dell'inserimento, nell'art. 156 lda, di tale clausola di salvezza, che in considerazione del fatto che il legislatore europeo, nell'affrontare la delicata questione delle responsabilità degli intermediari delle attività in rete, ha espressamente optato per un approccio di tipo "orizzontale", prescindente cioè dalla natura della violazione commessa con l'intermediazione tecnica del provider, diversamente da quanto avvenuto, ad esempio, negli Stati Uniti. Sul più volte citato approccio "orizzontale", che caratterizza la direttiva 2000/31 per quanto attiene alla responsabilità degli intermediari, si veda in dottrina, tra gli altri, COMANDE'-SICA, Il commercio elettronico, cit., 288 e ss

[86] Sia consentito il rinvio a BUGIOLACCHI, La responsabilità dell'host provider, cit., 189.

ha ritenuto che Youtube non sia tenuto a verificare preventivamente i video caricati, essendo materialmente impossibile controllare i 500 milioni di video messi a disposizione dagli utenti, con impostazione opposta a quella dei giudici italiani; o ancora, alla decisione con la quale la Corte di appello di Bruxelles, nel gennaio del 2010, ha effettuato rinvio pregiudiziale alla Corte di giustizia europea affinchè si pronunci sulla rispondenza o meno alla direttiva 2000/31 della imposizione di obblighi di controllo in capo ai provider.

In una tale situazione di incertezza normativa e giurisprudenziale è auspicabile, e forse improcrastinabile, un nuovo intervento del legislatore europeo, il quale, oltre ad "adeguare" la direttiva 2000/31 prevedendo procedure di notice and take down, secondo quanto disposto dallo stesso art. 21[87], consegni agli stati membri anche una meno vaga nozione di "conoscenza" dell'illecito, condizione necessaria affinchè possa scattare quell'obbligo di rimozione dei contenuti che, ove non adempiuto fa scaturire la responsabilità del provider di hosting.

La precisazione della nozione di "conoscenza" dell'illecito, unita alla previsione legale di una rapida procedura di comunicazione e rimozione dei materiali illeciti (che potrebbe avvenire con la cooperazione del titolare dei diritti lesi e del provider, come avviene, ad esempio, con il meccanismo VideoID, fornito da Google), potrebbe rappresentare il miglior strumento di balance tra i diritti degli isp, delle vittime di illeciti on line (sia che si riferiscano a violazione di diritti di proprietà intellettuale e dell'ingegno, che a lesioni di diritti della persona costituzionalmente protetti) e dei fruitori della rete, quale luogo di circolazione delle idee e condivisione della conoscenza, evitando l'attribuzione ai provider dell'inesigibile ruolo di censori telematici.

[87] A questo proposito è interessante osservare che la questione della individuazione delle procedure di notice and take down fosse stata affrontata anche in sede di "Prima relazione in merito all'applicazione della direttiva 2000/31", del 2003, nel cui ambito si evidenziò che la mancata previsione di tale procedura rappresentava un problema, anche in considerazione de fatto che gli stati membri avevano trovato difficoltà nel definire in tale materia quelle procedure autoprodotte dagli interessati menzionate anche nel considerando n. 40; per tali rilievi si veda anche CASSANO, Diritto dell'internet, Milano, 2005, 379 e ss.

Rivista elettronica di Diritto, Economia, Management

N. 1 - 2010 · pp. 68-88

Il diritto dell'informatica nella Società dell'Informazione. Profili giuridici ed interpretativi

Angela Viola

Abstract: Lo studio del diritto dell'informatica ha avuto di recente un impulso a partire dagli anni novanta in corrispondenza dello sviluppo tecnologico che ha portato alla definizione della c.d. Società dell'Informazione. Le nuove problematiche giuridiche ed interpretative che ne sono derivate hanno determinato un'evoluzione della tecnica normativa, in tutti i settori coinvolti. Dopo una panoramica relativa ai vari rapporti giuridici pubblicistici e privatistici, ci si sofferma sulla necessità di maggiore autonomia del diritto dell'informatica, attraverso la indispensabile codificazione normativa dei singoli settori.

The study of IT and Law recently gained a stronger impulse in the Italian legal system, since the 90's, as a consequence of the technological development, bringing to the definition of the so called Information Society. The new legal and interpretive problems that come with it, influenced the evolution of normative techniques in all the involved subject matters. After a framework on the different legal interactions in the public and private domains, the focus is on the necessity of more autonomy for the field of Law and IT, through a specific legislation, in the form of a code, of each sector.

Parole chiave: diritto dell'informatica, Società dell'Informazione, codificazione, tecniche normative, teoria dell'interpretazione.

Articolo pervenuto il 5 ottobre 2010, approvato il 23 novembre 2010

Introduzione

Lo studio del diritto dell'informatica può essere collegato a quegli aspetti giuridici e tecnico-giuridici relativi alle tecnologie dell'informazione e, nello specifico alla cd. società dell'informazione.
Se con l'informatica giuridica si è inteso fornire al diritto l'ausilio degli strumenti informatici, con il diritto dell'informatica si risponde all'esigenza, per certi aspetti complementare, di regolare giuridicamente fenomeni afferenti alla società digitale.
Il passaggio dall'informatica giuridica al diritto dell'informatica si è reso necessario dalla presenza di molteplici interventi legislativi avente ad oggetto la regolamentazione dei nuovi fenomeni afferenti alla Società dell'Informazione.
L'evoluzione tecnologica, ormai acclarata, ha affiancato all'informatica giuridica un insieme di materie con spiccate valenze applicative in ambito giuridico: il diritto dell'informatica diviene, per ricordare soltanto alcune branche, diritto delle tecnologie dell'informazione, comprendendo in tal modo il diritto civile e penale delle telecomunicazioni, diritto amministrativo delle reti, il diritto dei mezzi di informazione, il diritto d'autore sulle opere multimediali, il diritto e commercio elettronico, tutela dei dati personali.
In altri termini, se l'avvento del computer ha determinato, in una prima fase, l'evolversi della c.d. informatica giuridica, lo sviluppo delle comunicazioni elettroniche in genere ha comportato l'elaborazione di un <<diritto dell'informatica>> ossia un complesso di norme diretto a regolare la nuova realtà."[1] Questa è la ricostruzione che Ettore Giannantonio operava alla fine degli anni '80, proseguendo con l'affermare che il diritto dell'informatica dovesse consistere in una serie di istituti appartenenti ai vari campi del diritto. In tale prospettiva si poteva parlare allora di un diritto amministrativo, costituzionale, privato, penale, processuale e internazionale *dell'informatica*. Da questa rappresentazione l'autore derivava che ciascun ambito di diritto potesse essere trattato "soltanto dallo specialista di quel determinato settore[2]".
Quando Giannantonio scriveva le parole appena riportate l'ordinamento giuridico non aveva ancora conosciuto interventi aventi ad oggetto l'informatica, e la c.d. rivoluzione digitale era ancora ben lungi dal suo avvio, e l'incidenza delle tecnologie dell'informazione e della comunicazione sulla realtà socio-economica era ancora minima (in quell'epoca, tanto per fare un esempio, addirittura negli Stati Uniti Internet rappresentava ancora, prevalentemente, un network accademico).
Questo iniziale approccio sistematico e settoriale del diritto dell'informatica presentato dall'autore come quel complesso di norme legislative, di decisioni giurisprudenziali e di letteratura giuridica in materia, poneva già allora il problema dell'esistenza stessa e dell'opportunità di questa nuova materia del diritto e, conseguentemente della sua autonomia.
La discussione circa l'opportunità e la necessità di un intervento volto alla autonomia di

---

1 **Il presente scritto costituisce l'aggiornamento della relazione "Il rapporto tra il diritto e le nuove tecnologie dell'informazione e della comunicazione: il diritto dell'informatica" presentata al Convegno "L'informatica giuridica oggi", svoltosi il 1° dicembre 2005 presso la Facoltà di Giurisprudenza dell'Università di Roma "La Sapienza.*
GIANNANTONIO, Voce Informatica giuridica, Enciclopedia Giuridica Treccani, 1989.

2 idem

tale materia, risultava collegata, come lo stesso Giannantonio riferiva, al "riconoscimento legislativo" della particolare natura dell'attività automatizzata[3].
Il quadro è però radicalmente mutato, soprattutto dalla metà degli anni '90, con una velocità sempre più sorprendente.
Appare evidente che oggi, ad oltre vent'anni di distanza, questa impostazione vada rivisitata, alla luce dei numerosi cambiamenti che si sono registrati sia in ambito informatico, che economico, ed infine giuridico.

1. Evoluzione nell'ambito dell'informatica: alcuni esempi

Questa evoluzione non può stupire. Sotto il primo profilo, basti tener presente la cd. legge di Moore.
Gordon Moore, nel 1965, aveva constatato che la capacità dei microprocessori (chip) era pressoché raddoppiata ogni anno tra il 1959 ed il 1965: l'autore ipotizzò che tale tendenza avrebbe proseguito e così è stato. Nel 1975, lo stesso autore ha ridimensionato il ritmo di crescita a 18 mesi, per precisare poi, vent'anni dopo, nel 1995, che probabilmente la crescita della densità dei microprocessori e dunque la capacità delle prestazioni potrebbe raggiungere, nel 2017, il limite fisico della dimensione degli atomi[4].
In termini più semplici, la legge di Moore evidenzia che al crescere della potenza dei processori, il costo degli stessi diminuisce: con il passare del tempo, c'è una proporzione inversa tra le caratteristiche tecniche di performance ed il prezzo degli strumenti informatici, tanto più migliorano tali caratteristiche, tanto più si riduce il loro costo, secondo un'analisi economica della produzione.
La combinazione di questi due fattori ha determinato una rapidità nella diffusione del fenomeno che ha superato le aspettative iniziali, tanto che strumenti che inizialmente erano da considerarsi di esclusiva accessibilità da parte di pochi addetti ai lavori, sono oggi divenuti beni di consumo di utilizzo quotidiano.
Ad esempio, in Italia, possiamo riscontrare un evidente cambiamento nella percezione di tali strumenti informatici, che, in diversa misura, hanno conquistato uno spazio nel cd. paniere dei beni, tale da aver determinato già per il 2007/2008, tra i non addetti ai lavori, una copertura pari quasi al 50% rispetto all'acquisto di personal computer e, addirittura del 87,3%, rispetto all'acquisto di telefoni cellulari[5].
La Telefonia mobile è stabile ma il PC aumenta ancora quasi al 90% (87)

---

[3] [..] l'autonomia del diritto dell'informatica potrà essere affermata solo quando il legislatore abbia riconosciuto la particolare natura dell'attività automatizzata e abbia dettato una sua specifica disciplina; e quando la dottrina e la giurisprudenza abbiano prima indirizzato e quindi completato, ciascuna nel proprio ambito, l'attività del legislatore. Così GIANNANTONIO, Manuale di diritto dell'Informatica, Cedam ,2001, pag.9.

[4] v. PILATI e PERRUCCI (a cura di) Economia della conoscenza. Profili teorici ed evidenza empiriche, 2005, pag. 388 e ss.

[5] Il dato si riferisce all'acquisto di PC e di telefoni cellulari da parte delle famiglie italiane, come riferito dall'Annuario ISTAT 2009, Prospetto 11.4 pag. 296, reperibile sul sito http://www.istat.it/

Prospetto 11.4

Famiglie secondo il possesso di alcuni beni durevoli e ripartizione geografica - Anni 2007-2008 *(per 100 famiglie intervistate)*

BENI DUREVOLI	2007				2008			
	Nord	Centro	Mezzogiorno	Italia	Nord	Centro	Mezzogiorno	Italia
Lavastoviglie	47,8	50,5	25,8	41,3	49,4	49,4	28,0	42,5
Condizionatori d'aria	29,6	21,2	30,6	28,3	31,6	22,6	33,9	30,6
Fax	7,7	6,7	4,2	6,4	7,8	7,1	4,5	6,6
Segreteria telefonica	13,3	9,2	4,7	9,7	12,1	9,0	4,4	9,0
Telefono cellulare	86,3	88,8	83,1	85,8	87,7	90,4	84,7	87,3
Personal computer	48,5	49,0	40,2	45,9	50,8	51,7	43,6	48,7

A ciò va aggiunto che l'informatica stessa si è arricchita nel tempo di ulteriori elementi quali ad esempio la telematica[6] e la convergenza multimediale, che descrive la confluenza di comunicazione di dati e telecomunicazione (un tempo due mondi separati) in un'unica rete integrata con applicazioni e servizi nuovi. Ma non solo, lo sviluppo della tecnologica ha prodotto la trasformazione delle c.d. Reti di Nuova Generazioni (NGN) attraverso cui si sono sviluppate nuove modalità di creare conoscenza, di comunicare e di trasmettere informazioni. .[7]

L'evoluzione della convergenza multimediale attraverso la problematica delle c.d. Reti di Nuova Generazione (NGN) nasce proprio a seguito delle profonde trasformazioni nelle tecniche di trasmissione, basti pensare all'integrazione tra reti cellulari, reti digitali terrestri e reti satellitari e che, disponendo di una alta velocità trasmissiva compatibile con la rete Internet ed i servizi multimediali, consente di ricevere e trasmettere ogni genere di messaggi, compresi quelli radiotelevisivi. Le potenzialità delle NGN amplificano di fatto lo spettro delle comunicazioni elettroniche, si pensi per fare un esempio al VoIP (VoiceIP), trasformando in tal modo la modalità della comunicazione stessa.

Questa dinamica evolutiva del concetto di informatica configura la trasformazione della società, che oggi è divenuta a pieno titolo "Società dell'Informazione"[8].

---

[6] La parola telematica deriva dall'unione di due termini: telecomunicazioni e informatica. Pertanto indica l'utilizzo di tecnologie informatiche all'interno del settore delle telecomunicazioni. Le applicazioni della telematica hanno raggiunto moltissimi settori: basti pensare agli istituti bancari e ai Bancomat, ma anche ad Internet. Tutto ciò che riguarda la condivisione di informazioni e dati attraverso reti informatiche rientra nell'ambito della telematica.

[7] MORBIDELLI e DONATI, Comunicazioni: verso un diritto della convergenza? Torino, 2003. Vedi anche il recente Regolamento (UE, Euratom) n. 617/2010 del Consiglio, del 24 giugno 2010 , sulla comunicazione alla Commissione di progetti di investimento nelle infrastrutture per l'energia nell'Unione europea e che abroga il regolamento (CE) n. 736/96. Per un approfondimento sulle NGN si veda RUTKOWSKY, International Cooperation for the Protection of NGN Public Network Infrastructure, ITU WSIS Thematic Meeting on Cybersecurity, Ginevra, 2005.

[8] Il primo documento significativo a livello europeo del concetto di Società dell'Informazione è il cd. Rapporto Bangemann del 1994, che prende il nome dal Presidente della Commissione incaricata di redigere una relazione sulle infrastrutture da realizzare per lo sviluppo delle opportunità legate alla sfera della conoscenza e dell'informazione. La direttiva sul commercio elettronico n. 2000/31/CE individua la tipologia di servizi che riguardano la società dell'informazione al considerando n. 18, e ne determina la disciplina nell'articolato.

2. Caratteristiche della società dell'informazione

Per descrivere la Società dell'Informazione occorre far riferimento ai due concetti cardine che la connotano e che sono tra essi strettamente connessi: l'informazione e la comunicazione.
La coesione dei due concetti con l'ausilio delle nuove tecnologie ha trasformato il settore dell'IT (*Information Technology*) in ICT (*Information and Communication Technologies*) determinando, come si è visto, la trasformazione della società in Società dell'Informazione.
Le categorie distintive e peculiari di questo contesto possono essere sintetizzate nell' *a-territorialità*, *real-time* e *virtualità*.
L'*a-territorialità* rappresenta la mancanza di un vincolo di tipo territoriale e, di conseguenza statuale: infatti uno dei principi cardine, costituivi dell'ordinamento giuridico, quale la territorialità, perde la sua connotazione ontologica di fisicità divenendo nell'ambito della rete telematica un elemento virtuale.
Accanto alla perdita di fisicità spaziale, va registrata anche la mancanza di un riferimento temporale fisico: le transazioni ed ogni tipo di comunicazione avvengono *real-time*. Ciò significa che una volta realizzata la manifestazione di volontà ed il suo effetto tradotto in azione, lo spazio di tempo che normalmente intercorre tra la comunicazione della manifestazione di volontà stessa e la relativa ricezione viene ad essere annullato dalla tecnologia. La ricezione è virtualmente contestuale rispetto al momento della comunicazione, in altri termini comunicazione e ricezione avvengono nel cd. *tempo reale*, perché la tecnologia ha di fatto eliminato il tempo fisico della trasmissione che avviene in maniera simultanea ed immediata.
Se dunque lo spazio ed il tempo divengono un elemento virtuale, ciò solleva il problema dell'identificazione da parte dell'interprete del principio temporale e spaziale di riferimento giuridico: questo al fine di individuare la fattispecie giuridica, attraverso la sua qualificazione, e, di conseguenza, il diritto da applicare.
In termini economici, invece, il processo di integrazione delle cd. tecnologie dell'informazione e della comunicazione, richiede un intervento giuridico diretto a regolamentare il sistema socio-economico, visti gli imponenti interessi economici connessi allo sviluppo dell'innovazione tecnologica.
In questo caso, infatti, il diritto, e proprio il diritto dell'informatica, è chiamato a fornire un contributo rilevante, soprattutto anche rispetto allo stesso concetto di rete, dietro al quale sono forti gli interessi economici coinvolti.
Basti pensare, ad esempio, alle dimensioni delle cd. *reti transeuropee*, che devono consentire l'interconnessione tra gli Stati Membri in materia di trasporto, energia e telecomunicazioni, in prospettiva integrata, per ampliare e rafforzare il mercato interno, nel rispetto degli obiettivi della politica di coesione economica e sociale comunitaria ed all'interno di un quadro normativo di riferimento comune[9]. La politica relativa alle reti transeuropee era nata già alla metà degli anni '90, quando l'allora Comunità Europea contava ancora 15 Stati Membri: lo scenario che a partire dal 2004 si è presentato con l'allargamento e l'Europa a 27, ha richiesto

[9] V. in merito la Comunicazione della commissione COM(2003) 690: *Un'iniziativa europea per la crescita. Investire nelle reti e nella conoscenza per la crescita e l'occupazione.* Relazione finale al Consiglio Europeo, Bruxelles, 11.11.2003.

la revisione degli obiettivi politici e strategici, in modo da includere i nuovi Stati Membri, anche nello scenario dei Paesi dell'Europa Centro-Orientale (PECO).
La necessaria modifica della pianificazione sulle reti ha portato la Commissione ad un rafforzamento del mercato interno fondandolo sul principio del reciproco riconoscimento che garantisce la libera circolazione dei beni e dei servizi senza dover ricorrere all'armonizzazione delle legislazioni nazionali.
Alla luce di tali sviluppi appare evidente che il fenomeno tecnologico ed informatico necessiti di una disciplina trasversale che tenga conto delle specificità dei singoli canali del sistema di reti, mantenendo al tempo stesso una unitarietà di fondo.
Tutto ciò può essere assicurato soltanto dal riconoscimento dell'esistenza di una disciplina unitaria come il diritto dell'informatica.
A questi aspetti si aggiunge la profonda bipolarità e commistione tra il mezzo e lo strumento, che fa sì che la modalità di comunicazione si *fonda* e si *confonda* con il contenuto della comunicazione stessa, sollevando ancora non pochi nuovi problemi da un punto di vista sostanziale e formale per il giurista.

3. Le problematiche giuridiche della società dell'informazione

Fino a qualche tempo fa, l'approccio del giurista alle problematiche attinenti al diritto dell'informatica era di tipo settoriale e vi era una netta distinzione tra le discipline, nel tentativo di inquadrare in ciascuno particolare ambito una partizione dedicata agli aspetti dell'informatica nella sua applicazione specifica.
Questo si è tradotto in un metodo di interpretazione ed analisi che ha privilegiato l'impostazione tradizionale di specializzazione settoriale nelle diverse materie dove via via l'informatica ha fatto il suo ingresso, peraltro giustificata dalla stessa settorialità dei (rari) interventi normativi, caratterizzati da esigenze di elevata specificità, che non si prestavano ad un'opera di astrazione e concettualizzazione.
Tuttavia, non si può non tener conto della specificità del fenomeno informatico che è ravvisabile proprio nel fatto che esso determina la trasformazione della realtà, cambiando la prospettiva di riferimento in cui il diritto è chiamato ad intervenire.
Questo concetto aveva già trovato origine nel pensiero di Vittorio Frosini che, nel suo testo *Il Giurista e le tecnologie dell'informazione*, evidenziava la nascita del diritto soggettivo di libertà informatica, specificando che:
"Nel settore dell'informatica e nei suoi rapporti con il diritto, si è verificata una modificazione significativa nel corso di questi ultimi anni. […] al diritto è stato assegnato il compito di proteggere il singolo individuo, il soggetto giuridico nella sua individualità ed intimità, dalla invadenza del potere informatico, pubblico e privato; e questo è avvenuto mediante il

riconoscimento di un nuovo diritto soggettivo, chiamato la libertà informatica." [10]
Oggi, quindi, il diritto dell'informatica richiede in modo incontestabile di essere ripensato e costruito come nuova disciplina nell'ambito dell'esperienza giuridica, in una prospettiva collegata ed integrata all'informatica giuridica.
L'esigenza di vedere tutelato il diritto dell'informatica con una autonoma impostazione metodologica ed epistemologica e, dunque necessariamente anche didattica, nasce dalla profonda pervasività del fenomeno informatico nella società contemporanea, che pone il giurista davanti ad un interrogativo di fondo: la normazione del fenomeno informatico e delle relazioni tra informatica e diritto necessita di nuove regole o è sufficiente adattare gli strumenti già esistenti, attraverso il ricorso all'interpretazione estensiva, all'analogia ed ai principi generali?
Da un punto di vista metodologico, ci si chiede quali siano le argomentazioni a favore dell'una impostazione o dell'altra in termini di politica legislativa in ambito di diritto dell'informatica e quali conseguenze rispettivamente possano derivare.
Se qualifichiamo questi fenomeni come fattispecie del tutto nuove rispetto al quadro giuridico di riferimento, è chiaro che risulta necessario intervenire autonomamente attraverso la costruzione di nuove regole con la relativa codificazione.
Ciò significherebbe creare *ex novo* delle qualificazioni giuridiche per ciascun fenomeno che faccia in qualche modo riferimento all'impiego di tecnologie informatiche, sia nell'ambito privatistico, che pubblicistico.
Conseguentemente, una tale impostazione determinerebbe la creazione di una nuova *sistematica del diritto*, in base alla quale le categorie generali che afferiscono ad ogni ordinamento giuridico dovrebbero essere riviste, ripensate e riscritte alla luce dei nuovi fenomeni.
Se così fosse, dovremmo immaginare, tanto per fare un esempio, all'introduzione, accanto alla disciplina di diritto comune dei contratti, contenuta nel codice civile, una disciplina del contratto telematico**.**
Questo non è possibile, perché anche in presenza di strumenti informatici e telematici, la qualificazione normativa delle singole categorie giuridiche rimane la stessa: manteniamo lo stesso esempio del contratto.
Il contratto tradizionale ed il contratto informatico sono entrambi costituiti dall'elemento comune di proposta ed accettazione, l'elemento che li differenzia, invece, risiede nella modalità di realizzazione. Basta la differente modalità di realizzazione dei presupposti costitutivi del contratto a giustificare la modifica della natura giuridica e l'attribuzione di un nuovo *nomen juris*?
Ebbene, sembra che tale soluzione non sia né opportuna né necessaria.
Possiamo allora ipotizzare che i fenomeni afferenti alla Società dell'Informazione possono essere disciplinati utilizzando le categorie giuridiche tradizionali, in quanto le nuove modalità di svolgimento dei rapporti non modificano la loro essenza. Un iniziale approccio comunitario era infatti proprio in questa direzione, la Commissione Europea già nel 1996 aveva decretato che " ciò che è illecito fuori della Rete è altrettanto illecito nella Rete stessa".

[10] FROSINI Il Giurista e le tecnologie dell'informazione, Roma, 1998, pag. 43.

A ben vedere, però, le nuove tecnologie hanno imposto di verificare la tenuta delle regole già esistenti; queste ultime, non sempre sono state in grado di disciplinare le nuove modalità di realizzazione di attività giuridica tradizionale. Pensiamo per esempio al documento informatico: è evidente che le caratteristiche di tale documento hanno determinato la necessità di un intervento normativo volto alla specificazione del soggetto da cui il documento proviene e delle altre condizioni che ne garantiscano la paternità, l'immodificabilità ed integrità.
La conferma di ciò si può trovare nell'evoluzione stessa del diritto: si pensi al contratto concluso fuori dei locali commerciali[11] ed al cd. contratto a distanza[12], che costituiscono il precedente logico per la disciplina dei contratti realizzati attraverso la rete telematica. Con riferimento ad essi il legislatore, ben lungi dal creare un nuovo titolo giuridico, ha ritenuto invece necessario formulare una disciplina *ad hoc*, che tenesse conto delle specifiche caratteristiche che rimanevano sfornite di tutela adattando i principi della disciplina del contratto tradizionale.
Allo stesso modo, il legislatore si è posto di fronte al problema più specifico dell'individuazione temporale del momento della conclusione del contratto tramite Internet, per stabilirne l'efficacia e la rilevanza giuridica.
Per ricondurre un effetto giuridico equiparato agli elementi tradizionali di proposta ed accettazione, attraverso il mezzo telematico, il legislatore ha utilizzato la *fictio juris* del riferimento alla mera possibilità di accesso alle comunicazioni contenenti proposta ed accettazione. Recita infatti l'art. 13 del d. lgs. 70/2003 (comma 3): "L'ordine e la ricevuta si considerano pervenuti quando le parti alle quali sono indirizzati hanno la possibilità di accedervi."
In questo modo il legislatore non ha fatto altro che integrare con una disciplina specifica quegli aspetti che non trovavano adeguata tutela attraverso gli strumenti tradizionali.
La nuova normativa è pur sempre agganciata alla tradizione dell'ordinamento: essa va interpretata alla luce dei principi generali del diritto.
Ecco quindi che non è possibile stravolgere l'ordinamento esistente attraverso l'adozione di norme nuove totalmente sradicate dal contesto giuridico di riferimento, ma è necessario che la normazione sui nuovi fenomeni avvenga considerando tutto il sistema nel suo insieme.
Conseguentemente, l'effetto che il fenomeno specifico produce *in modo diverso* va considerato dal giurista *in modo diverso* secondo gli strumenti dell'interpretazione: tale diversità nella modalità di verificazione non deve inficiare l'effetto giuridico, che rimane pur sempre lo stesso.
Come rendere giuridicamente possibile e valida questa identità di effetto rispetto alla diversità di realizzazione?
Attraverso gli strumenti della teoria dell'interpretazione: in particolare, se da una parte l'argomento analogico pone in essere attraverso la ricerca dell'*eadem ratio,* la vera e propria norma del caso concreto, volta a disciplinare l'ipotesi non prevista in precedenza, l'interpretazione estensiva, viceversa, estende ed amplia la *ratio* di una norma già esistente fino a farle ricomprendere e disciplinare anche il caso non previsto.
Quale che sia lo strumento prescelto, occorre, in definitiva confrontarsi con il fatto che il

---

[11] v. Decreto Legislativo 15.01.1992, n. 50 in attuazione della direttiva 85/577/CEE, in materia di contratti negoziati fuori dei locali commerciali.

[12] v. Decreto Legislativo 22.05.1999, n. 185, in attuazione della Direttiva 1997/7/CE, relativa alla protezione dei consumatori in materia di contratti a distanza.

problema del giurista non è tanto di qualificare la regola da applicare, ma di trovare una normazione idonea per l'organizzazione del fenomeno stesso.
L'autonomia della disciplina acquista la sua giustificazione proprio comprendendo l'univocità del fenomeno in sé, che implica la necessità di una univoca gestione della sua evoluzione, assicurabile soltanto attraverso la conoscenza dei rapporti di interferenza ed intersezione tra informatica e diritto.
Ad esempio la virtualità impone talvolta di risolvere il problema dell'individuazione della giurisdizione in rete. L'iniziale difficoltà di accertare lo Stato competente per la risoluzione di eventuali controversie che appariva insormontabile, con riferimento al commercio elettronico, è stata in parte risolta attraverso l'applicazione del criterio di collegamento al luogo di stabilimento del soggetto prestatore del servizio e non alla collocazione fisica delle tecnologie di supporto informatico[13]. Tutto questo potrebbe essere ricondotto alla mera applicazione in via analogica di un criterio di collegamento del diritto internazionale privato: invero, si tratta di qualcosa di più. Il giurista grazie all'analisi del fenomeno nei suoi aspetti tecnologici ed economici, ha operato una scelta ben precisa prediligendo la tutela del soggetto debole, all'interno della contrattazione telematica.
Infine, vi sono alcuni fenomeni del tutto inediti rispetto alla sistematicità dell'ordinamento: si pensi alla qualificazione giuridica dello spazio cibernetico in sé, oppure alla difficoltà di intendere il concetto di privacy con riferimento alla comunicazione elettronica, proprio perché quest'ultima presenta aspetti profondamente innovativi rispetto alla comunicazione tradizionale, o ancora alle problematiche della convergenza multimediale che coinvolgono profili giuridici interdisciplinari.
Rispetto a tali fenomeni, il coordinamento dello studioso di diritto dell'informatica appare estremamente utile a *configurare il sistema* giuridico, nel senso che la sua percezione del fenomeno informatico e tecnologico serve a comprendere la direzione da prendere per la disciplina giuridica.

4. Evoluzione della tecnica normativa

Da un punto di vista storico, in Italia la scelta rispetto all'interrogativo circa il fondamento autonomo del diritto dell'informatica è stata determinata da una *maturazione* nella comprensione del fenomeno informatico economico e sociale.
All'inizio è stato tentato, come abbiamo visto, un processo interpretativo ed analogico, anche perché tale processo appariva più consono alla necessità di risolvere nell'immediato le problematiche sollevate dalle nuove realtà.
Nella stessa ottica è intervenuta, ad esempio, la prima normativa in tema di criminalità e reati informatici, che è stato, per alcuni anni, l'unico testo normativo contenente una definizione di documento informatico. In questo caso, il legislatore ha introdotto delle fattispecie di reato nuove, che tuttavia si ricollegano, nell'oggetto giuridico di tutela e nelle caratteristiche

[13] v. Direttiva 2000/31/CE e relativa attuazione in Italia con il Decreto Legislativo n. 70/2003.

delle fattispecie costituenti reato, al principio di tassatività e di legalità, categorie generali e fondamento del diritto penale.
In termini privatistici, allo stesso modo, si è posto il problema di definire il documento informatico: il legislatore in un primo tempo lo ha equiparato ai fini giuridici a quello cartaceo, in ordine alla efficacia e validità dello stesso. Successivamente è stato necessario creare delle norme che potessero individuare le modalità giuridicamente rilevanti per la creazione e validazione del documento informatico stesso e questo è avvenuto, anche sulla spinta della normativa comunitaria, attraverso la legislazione primaria e le norme tecniche di dettaglio in tema di firma digitale.
Ciò fa riflettere sul concetto che le caratteristiche della Società dell'Informazione hanno di fatto richiesto una innovazione normativa, basata pur sempre sui principi generali insiti nell'ordinamento.
Anche con riferimento alla tutela del consumatore, che nasce dall'esigenza di far fronte ad alcune particolari ipotesi di contrattazione, la cui caratteristica fondamentale è la posizione di debolezza del contraente consumatore, si sono aggiunte delle ulteriori esigenze con l'avvento della digitalizzazione.
In proposito, ad esempio, partendo dal d. lgs.185/99, che recepisce la tutela del consumatore nello specifico ambito della contrattazione a distanza, per quanto qui non si tratti di contrattazione informatica in senso stretto, la tecnica adottata dal legislatore è stata quella di estendere tale disciplina al cd. consumatore informatico. A tale disciplina va aggiunta quella relativa al Codice del Consumo (D.Lgs. 206/2005) che riunisce in un unico testo le disposizioni di 21 provvedimenti (4 leggi, 2 DPR, 14 D.Lgs. e 1 regolamento di attuazione) sintetizzando in 146 articoli il contenuto di 558 norme (utilizzando lo strumento della c.d. *"semplificazione organica"*).
La categoria dei contratti a distanza ha poi trovato una sua più specifica definizione e collocazione, più strettamente collegata all'ambito informatico, nella direttiva comunitaria 2000/31 relativa proprio al commercio elettronico, e nel suo decreto di recepimento d.lgs. 70/2003, a livello dell'ordinamento italiano.
Vedremo poi in ambito pubblicistico come invece la scelta del legislatore sia stata volta alla codificazione creando in tal modo una normativa omogenea e coesa.

5. Aree tematiche

Le aree tematiche implicate da questo processo di sviluppo possono essere suddivise principalmente nei due tradizionali settori del diritto: il privato e il pubblico.
Da una parte si riscontra l'esigenza di legittimare i rapporti informatici: documento informatico, firma digitale, contratti telematici, e verificare le possibilità di tutela approntate dal legislatore rispetto a software, banche dati, privacy, etc.
Dall'altra emerge l'esigenza della pubblica amministrazione di adeguarsi all'evoluzione tecnologica.
Ad esempio, nella suddivisione tra i due settori si possono individuare alcune materie già oggetto di normativa fin dai primi anni '90 ed altre che si vanno delineando in questi ultimi anni.

PRIVATO	PUBBLICO
Documento informatico e firma digitale. Fatturazione elettronica	Codice dell'Amministrazione digitale
Commercio elettronico: direttiva comunitaria e decreto legislativo attuativo. Responsabilità civile informatica.	Procedimento amministrativo elettronico, appalti amministrativi informatici (e-procurement)
Tutela del consumatore	Archiviazione ottica dei documenti informatici (protocollo informatico, mandato di pagamento elettronico –
Tutela della privacy. Diritto d'Autore. Tutela del software e banche dati. Nomi di dominio.	Processo telematico. Reati informatici
Posta elettronica certificata	

6. La nuova codificazione pubblicistica: la ratio ed il ruolo del diritto dell'informatica.

Nella struttura di questo lavoro, concentriamo a questo punto la nostra attenzione sulle innovazioni normative in materia pubblicistica.
A questo proposito due sono gli aspetti preponderanti per l'esame della normativa pubblicistica recente.
Un primo elemento che risalta è che, sia a livello normativo che amministrativo, la scelta di politica legislativa si impernia sull'esigenza di semplificazione, che costituisce il principio fondante del riassetto normativo e della "nuova" codificazione.
Infatti, la legge 229/2003, art. 1 comma 3, dispone che:
"Salvi i principi e i criteri direttivi specifici per le singole materie, stabiliti con la legge annuale di semplificazione e riassetto normativo, l'esercizio delle deleghe legislative di cui ai commi 1 e 2 si attiene ai seguenti principi e criteri direttivi:
a) definizione del riassetto normativo e codificazione della normativa primaria regolante la materia, previa acquisizione del parere del Consiglio di Stato, reso nel termine di novanta giorni dal ricevimento della richiesta, con determinazione dei principi fondamentali nelle materie di legislazione concorrente"[14].
È un indirizzo nuovo che ben si aggancia alle peculiarità della tecnologia informatica.
Infatti, accanto a questo aspetto di tecnica normativa, non può essere trascurato l'elemento legato all'evoluzione tecnologica ed all'innovazione della società digitale.

[14] v. Legge 29 luglio 2003, n.229 Interventi in materia di qualità della regolazione, riassetto normativo e codificazione. - Legge di semplificazione 2001. (GU n. 196 del 25-8-2003 - testo in vigore dal 9-9-2003): L'art. 1 (Riassetto normativo e codificazione) sostituisce l'articolo 20 della Legge 15 marzo 1997, n. 59, e successive modificazioni.

La scelta normativa improntata sulla fattispecie della codificazione può essere letta, con riferimento all'oggetto della nostra materia, proprio come risposta all'esigenza di organizzare in modo unitario la disciplina giuridica della società dell'informazione.
Difatti il legislatore è passato dalla originaria impostazione di delegificazione, volta alla riduzione nell'ordinamento delle fonti di rango primario nelle materie oggetto della semplificazione, ad una vera e propria nuova codificazione, volta, di contro, alla formazione di una disciplina organica proprio di rango primario.
Ancor più, se si accoglie l'interpretazione del Consiglio di Stato, nel Parere del Febbraio 2005[15], si può parlare addirittura di "rilegificazione" di molte norme, che sono state trasformate gerarchicamente dall'intervento di codificazione, da norme di rango secondario a norme di rango primario.
Una conseguenza di questa nuova forma di tecnica legislativa, si può ravvisare ad esempio nel cd. *Codice della privacy*[16] in cui normazione di carattere regolamentare, quale il regolamento n. 318/99[17], relativo alle misure di sicurezza nel trattamento dei dati personali, è stato assorbito e ricompreso nel citato Codice, in modo che le disposizioni in esso contenute hanno assunto piena efficacia di fonte primaria.
Questa impostazione di carattere legislativo rappresenta, proprio per il diritto dell'informatica una riprova dell'acquisizione di una sempre maggiore rilevanza ed autonomia: infatti, il passaggio di determinate disposizioni da fonti di rango secondario a fonti di rango primario, rappresenta un evidente riconoscimento della materia come ambito organico, unitario ed autonomo.
Tuttavia, ci si è chiesti come vada interpretata questa nuova forma di "codificazione": se essa possa essere qualificata come nuovo corpus normativo unitario, con i caratteri propri della generalità ed astrattezza di un codice organico, oppure all'opposto come vera e propria forma di "decodificazione"[18] in cui il legislatore prende atto della impossibilità di una uniforme tutela codicistica tradizionale rispetto a problematiche giuridiche emergenti.
In altri termini, questa scelta di politica legislativa può essere letta in chiave positiva o negativa, poiché l'esigenza di codificazione può essere intesa come forma di risposta ad un principio sistematico e di garanzia nei confronti dello Stato, ma anche come limite del sistema stesso.
La ratio giustificatrice di tali interventi normativi può essere rilevata nella necessità di introdurre la disciplina di determinate materie nuove, non regolate prima e dove, proprio per la novità, le fonti non possono essere individuate attraverso il mero ricorso agli strumenti dell'interpretazione analogica.
È chiaro che l'intento del legislatore è diretto verso una normazione il più possibile unitaria della materia.
Proprio in questa prospettiva è possibile rielaborare oggi il significato delle grandi codificazioni

---

[15] v. Parere C.d.Stato del 7 Febbraio 2005, n. 11995, punto 9.

[16] Decreto Legislativo n. 196 del 30 giugno 2003, denominato "Codice in materia di protezione dei dati personali".

[17] Decreto del Presidente della Repubblica 28 luglio 1999, n.318: Regolamento recante norme per l'individuazione delle misure minime di sicurezza per il trattamento dei dati personali, a norma dell'articolo 15, comma 2, della legge 31 dicembre 1996, n. 675, pubbl. sulla GU n. 216 del 14-9-1999.

[18] Per un'analisi del problema si veda IRTI, L'età della decodificazione, Milano, 1979.

dell'800 in cui i codici " si presentano, tradizionalmente, come fonti di diritto generale, in antitesi con il diritto contenuto nelle altre leggi, che rispetto ai codici si sogliono definire come leggi speciali, fonti di diritto speciale"[19].

È proprio alla luce di questa ricostruzione che è possibile agganciare tale problematica alle nuove prospettazioni che afferiscono anche al diritto dell'informatica.

Casi emblematici, nell'ambito della materia sistematica riconducibile al diritto dell'informatica, sono ad esempio, il citato *Codice della privacy* per quanto riguarda la protezione dei dati personali, il *Codice sulle comunicazioni elettroniche*[20], che ha rappresentato un intervento di riforma sul precedente codice postale[21] risalente agli anni '30, ed, anche la normativa in materia del *Codice dell'Amministrazione digitale*[22], il cui carattere innovativo si ravvisa nella formalizzazione/istituzionalizzazione del nuovo mezzo della comunicazione elettronica da parte del cittadino nei confronti delle pubbliche amministrazioni e all'interno delle pubbliche amministrazioni stesse. A ciò va aggiunto anche il *Codice del Consumo*[23] che come già riferito rappresenta un esempio di coordinazione normativa delle disposizioni relative alle definizioni di consumatore, professionista, venditore, produttore. Le regole raccolte nel "Codice" sono tutte di matrice e di competenza statale. La vigente formulazione dell'articolo 117 Cost., dopo la riforma del Titolo V, riconosce il ruolo essenziale della legislazione statale in materia di disciplina del processo unitario del consumo, nella prospettiva della finalità di tutela del consumatore.

Si tratta di una tecnica legislativa sistematica che permette di ordinare per settori organici le singole materie di riferimento, con le rispettive caratteristiche, individuando volta per volta i diritti afferenti ad ogni singolo contesto, con gli strumenti di tutela nei confronti dei consociati e dell'ordinamento stesso.

Infatti, il significato profondo della codificazione è collegato non solo alla esigenza di affermare un principio di statualità dell'ordinamento giuridico, ma anche e soprattutto, di vedere confermato e garantito il principio fondamentale di uguaglianza.

Tale principio va rivisitato e reinterpretato alla luce della innovazione tecnologica.

In questa prospettiva, la scelta del codice anziché di un semplice testo unico di mero coordinamento può conferire alla materia codificata una diversa accezione e dunque un nuovo valore di organicità: il diritto dell'informatica può in questo processo evolutivo essere inteso come ambito normativo unitario, dove tutte le norme ad esso collegate risultano connesse dall'elemento informatico.

In tale chiave vanno letti ad esempio, con riferimento al Codice dell'Amministrazione digitale, i principi che delineano il dialogo tra privato e PA e delle PA tra loro. L'art. 3 del citato codice, infatti stabilisce che "I cittadini e le imprese hanno diritto a richiedere ed ottenere l'uso delle tecnologie telematiche nelle comunicazioni con le pubbliche amministrazioni centrali e con i

---

19 GALGANO, Trattato di Diritto Civile e Commerciale, Vol. I, Padova, 1999, pag. 70.

20 Decreto Legislativo 1 agosto 2003, n. 259 di recepimento delle direttive 2002/19/CE (direttiva accesso), 2002/20/CE (direttiva autorizzazioni), 2002/21/CE (direttiva quadro) e 2002/22/CE (direttiva servizio universale), recante il "Codice delle comunicazioni elettroniche", pubblicato sulla G.U. n. 214 del 15 settembre 2003.

21 Codice Postale, approvato con R.D. 27 febbraio 1936, n. 645.

22 Decreto legislativo del 7 marzo 2005, n. 82, pubblicato sulla G.U. n. 111 del 16 maggio 2005.

23 Decreto legislativo del 6 settembre 2005 n. 206.

gestori di pubblici servizi statali nei limiti di quanto previsto nel presente codice". Ancora, l'art. 4 sancisce il principio generale di partecipazione al procedimento amministrativo informatico. Sono questi i principi e gli strumenti attraverso i quali si è garantito lo sviluppo relativo al percorso di semplificazione amministrativa già avviato con la legge sul procedimento amministrativo n. 241/90, arricchito dei profili attinenti alle modalità della comunicazione elettronica e quindi della innovazione tecnologica.
Fondamentale, al riguardo, è l'art. 12 del citato codice[24], che evidenzia come le caratteristiche peculiari del procedimento amministrativo, e gli obiettivi di efficienza, efficacia, economicità, imparzialità, trasparenza, semplificazione e partecipazione, sono perseguiti attraverso l'utilizzazione delle ICT.
La peculiarità della comunicazione elettronica con la Pubblica Amministrazione permette inoltre di evidenziare come la normativa di rango primario necessiti comunque, in questo particolare ambito caratterizzato dalla continua innovazione tecnologica, di una forma di intervento regolatorio dinamico e flessibile[25].

7. Lineamenti dei nuovi rapporti tra privato e Pubblica Amministrazione digitale: breve rassegna normativa

Una parte copiosa del diritto dell'informatica oggi, grazie anche all'intervento normativo del Codice dell'amministrazione digitale viene ridefinita in modo organico per quanto attiene i principi in materia di organizzazione della PA in un'ottica di riforma "strutturale e gestionale"[26],

---

[24] v. art. 12 d. lgs. 82/05 (*Norme generali per l'uso delle tecnologie dell'informazione e delle comunicazioni nell'azione amministrativa*):
1. Le pubbliche amministrazioni nell'organizzare autonomamente la propria attività utilizzano le tecnologie dell'informazione e della comunicazione per la realizzazione degli obiettivi di efficienza, efficacia, economicità, imparzialità, trasparenza, semplificazione e partecipazione.
2. Le pubbliche amministrazioni adottano le tecnologie dell'informazione e della comunicazione nei rapporti interni, tra le diverse amministrazioni e tra queste e i privati, con misure informatiche, tecnologiche, e procedurali di sicurezza, secondo le regole tecniche di cui all'articolo 71 .
3. Le pubbliche amministrazioni operano per assicurare l'uniformità e la graduale integrazione delle modalità di interazione degli utenti con i servizi informatici da esse erogati, qualunque sia il canale di erogazione, nel rispetto della autonomia e della specificità di ciascun erogatore di servizi.
4. Lo Stato promuove la realizzazione e l'utilizzo di reti telematiche come strumento di interazione tra le pubbliche amministrazioni ed i privati.
5. Le pubbliche amministrazioni utilizzano le tecnologie dell'informazione e della comunicazione, garantendo, nel rispetto delle vigenti normative, l'accesso alla consultazione, la circolazione e lo scambio di dati e informazioni, nonché l'interoperabilità dei sistemi e l'integrazione dei processi di servizio fra le diverse amministrazioni nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71 .

[25] Tutto ciò è assicurabile attraverso il ricorso ad una normativa di rango secondario: a tale proposito, il parere del Consiglio di Stato in ordine al Codice in questione, ha evidenziato che "il Governo può in ogni momento avvalersi della propria potestà normativa secondaria, che è una potestà autonoma e non "delegata". Così il Parere C.d.Stato del 7 Febbraio 2005, cit. punto 9.

[26] Così l'art. 15 d.lgs. 82/05: (Digitalizzazione e riorganizzazione)
1. La riorganizzazione strutturale e gestionale delle pubbliche amministrazioni volta al perseguimento degli obiettivi di cui all'articolo 12 , comma 1 , avviene anche attraverso il migliore e più esteso utilizzo delle tecnologie dell'informazione e della comunicazione nell'ambito di una coordinata strategia che garantisca il coerente sviluppo del

sia a livello centrale che locale, per quanto consentito dalla riforma del Titolo V: infatti l'art. 14 del codice fa esplicito riferimento all'attuazione del disposto dell'articolo 117, secondo comma, lettera r)[27]. Di rilievo appare in questo ambito il concetto di *coordinamento informatico dei dati*, per la prima volta il legislatore utilizza una definizione così specifica e strettamente collegata alla realtà della società dell'informazione, la cui portata è stata oggetto di analisi da parte della sentenza della Corte costituzionale 7 luglio 2005, n. 271. In tale ambito la Corte si è occupata di individuare e delimitare l'ambito della potestà legislativa esclusiva attribuita allo Stato nel settore che qui ci interessa[28].

Ma di ancor più evidente interesse per il giurista appaiono le disposizioni che riguardano i rapporti tra i privati e la pubblica amministrazione: si è già fatto riferimento ai principi desumibili dal diritto all'uso delle tecnologie (cit. art. 3 d. lgs. 82/05), alla partecipazione all'iter procedimentale amministrativo (cit. art. 4 id.). Va evidenziato, inoltre, come il legislatore ha soffermato l'attenzione sul concetto di partecipazione alla cd. democrazia elettronica (art. 9 id.[29]).

Questa disposizione apre una prospettiva programmatica di indirizzo e coordinamento per la futura normazione in materia: difatti, la stessa contiene un evidente riferimento al principio di partecipazione democratica in una nuova chiave di lettura che è quella legata alla digitalizzazione della società dell'informazione.

Inoltre, è possibile evidenziare, da una diversa angolazione, come il riconoscimento di tale diritto sottolinei ancora una volta la necessità di considerare la materia del diritto dell'informatica come espressione normativa autonoma rispetto al passato.

Mentre infatti i primi interventi normativi sono stati caratterizzati da una impostazione di

processo di digitalizzazione.

2. In attuazione del comma 1, le pubbliche amministrazioni provvedono in particolare a razionalizzare e semplificare i procedimenti amministrativi, le attività gestionali, i documenti, la modulistica, le modalità di accesso e di presentazione delle istanze da parte dei cittadini e delle imprese, assicurando che l'utilizzo delle tecnologie dell'informazione e della comunicazione avvenga in conformità alle prescrizioni tecnologiche definite nelle regole tecniche di cui all'articolo 71 .

3. La digitalizzazione dell'azione amministrativa è attuata dalle pubbliche amministrazioni con modalità idonee a garantire la partecipazione dell'Italia alla costruzione di reti transeuropee per lo scambio elettronico di dati e servizi fra le amministrazioni dei Paesi membri dell'Unione europea.

[27] Il testo dell' art. 14 (Rapporti tra Stato, Regioni e autonomie locali) è il seguente:

1. In attuazione del disposto dell'articolo 117, secondo comma, lettera r), della Costituzione, lo Stato disciplina il coordinamento informatico dei dati dell'amministrazione statale, regionale e locale, dettando anche le regole tecniche necessarie per garantire la sicurezza e l'interoperabilità dei sistemi informatici e dei flussi informativi per la circolazione e lo scambio dei dati e per l'accesso ai servizi erogati in rete dalle amministrazioni medesime.

2. Lo Stato, le regioni e le autonomie locali promuovono le intese e gli accordi e adottano, attraverso la Conferenza unificata, gli indirizzi utili per realizzare un processo di digitalizzazione dell'azione amministrativa coordinato e condiviso e per l'individuazione delle regole tecniche di cui all'articolo 71 .

3. Lo Stato, ai fini di quanto previsto ai commi 1 e 2, istituisce organismi di cooperazione con le regioni e le autonomie locali, promuove intese ed accordi tematici e territoriali, favorisce la collaborazione interregionale, incentiva la realizzazione di progetti a livello locale, in particolare mediante il trasferimento delle soluzioni tecniche ed organizzative, previene il divario tecnologico tra amministrazioni di diversa dimensione e collocazione territoriale.

[28] V. Corte cost., 7 luglio 2005, n. 271, reperibile sul sito www.cortecostituzionale.it .

[29] Il testo dell'art. 9 (Partecipazione democratica elettronica) del citato d. lgs. così dispone:

1. Lo Stato favorisce ogni forma di uso delle nuove tecnologie per promuovere una maggiore partecipazione dei cittadini, anche residenti all'estero, al processo democratico e per facilitare l'esercizio dei diritti politici e civili sia individuali che collettivi.

tipo settoriale e sporadico, negli ultimi anni, invece, si può registrare sempre più un approccio normativo sistematico e coordinato.
Questo rappresenta un'evoluzione non solo dello strumento tecnico normativo, come tentativo di risposta alla situazione storica di crisi della legge[30], ma anche, dal punto di vista sostanziale, un chiaro segnale di individuazione della materia del diritto dell'informatica.
In tale ottica, vanno lette le previsioni sostanziali e procedurali del nuovo codice, che pongono il cittadino nella condizione di poter utilizzare gli strumenti informatici in un regime uniformemente regolato in base al nuovo codice.
Infatti, in primo luogo, il legislatore ha ribadito il concetto della equivalenza giuridica del documento informatico a tutti gli effetti a quello cartaceo, come già era stato previsto dal principio introdotto con l'art. 15 comma 2 l. 59/97, rimettendo alle regole tecniche, e dunque ad una regolamentazione di dettaglio, la definizione delle caratteristiche per la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione temporale dei documenti informatici.
Allo stesso modo, si richiama la disciplina della materia della firma digitale, in parte risolvendo i problemi applicativi derivanti dall'interpretazione dell'art. 6 della l. 10/2002, che modificava l'art. 10 del T.U. n. 445/2000 "Forma ed efficacia del documento informatico" oggi abrogato dall'articolo 75 del decreto legislativo n. 82 del 2005. La nuova normativa di riferimento chiarisce il significato e la validità del documento informatico e della firma digitale, rispetto alla normativa precedente, con un assetto sistematico di carattere primario, unitario e coeso.
Nel dialogo di comunicazione tra le PA e tra le Amministrazioni ed i privati, assume un ruolo sicuramente centrale la disciplina relativa alla *posta elettronica* ed, in particolare la posta elettronica *certificata*.
Lasciando da parte il dibattito teorico sulla qualificazione giuridica della comunicazione attraverso la posta elettronica in generale, la valenza dell'introduzione di tale strumento tecnologico, in questo dialogo, come veicolo di trasmissione di documenti con piena efficacia di legge, ove siano rispettati i requisiti tecnici previsti, riflette l'esigenza di vedere tutelata la comunicazione in via elettronica.
Infatti, nella prospettiva di una società digitalizzata, la comunicazione a mezzo di posta elettronica diviene la "norma": recita l'art. 47 (Trasmissione dei documenti attraverso la posta elettronica tra le pubbliche amministrazioni) al comma 1:
"Le comunicazioni di documenti tra le pubbliche amministrazioni avvengono di norma mediante l'utilizzo della posta elettronica; esse sono valide ai fini del procedimento amministrativo una volta che ne sia verificata la provenienza."
Questo principio di carattere generale, trova il suo corollario nel successivo art. 48 (Posta elettronica certificata) che dispone (comma 1):
"La trasmissione telematica di comunicazioni che necessitano di una ricevuta di invio e di una ricevuta di consegna avviene mediante la posta elettronica certificata ai sensi del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68.[31]"

---

[30] MODUGNO-CELOTTO-RUOTOLO, Considerazioni sulla crisi della legge, in Studi Parlamentari e di Politica Costituzionale, 1999, 125-126, pp. 7 ss.

[31] Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27

Ciò ha permesso di avvalorare il ruolo giuridico delle tecnologie nella società dell'informazione. Un cenno, infine, meritano le disposizioni in materia di siti delle Pubbliche Amministrazioni, che stabiliscono delle indicazioni uniformi per tutte le Pubbliche Amministrazioni Centrali, sia sulle modalità di realizzazione tecnica, nel rispetto dei principi di accessibilità, usabilità e reperibilità, anche da parte delle persone disabili, completezza di informazione, chiarezza di linguaggio, affidabilità, semplicità di consultazione, qualità, omogeneità ed interoperabilità, sia quanto ai contenuti necessari da inserire.
Attraverso la veicolazione informatica si rende pertanto fruibile molto più velocemente il servizio pubblico all'utente, che esercita pertanto il proprio diritto ad essere informato ed a poter prendere conoscenza autonomamente dei dati che lo riguardano o che lo interessano: in questo modo, attraverso l'utilizzo dello strumento di Internet e la diffusione della comunicazione elettronica, il diritto di libertà informatica viene inteso nell'accezione di pretesa di libertà in senso attivo " non libertà da, ma libertà di, che è quella di valersi degli strumenti informatici per fornire ed ottenere informazioni di ogni genere"[32].

Considerazioni conclusive

Al termine di questa rassegna, che dovrebbe aver dato il senso delle profonde innovazioni apportate al nostro ordinamento dall'avvento delle tecnologie dell'informazione e della comunicazione, è forse possibile esprimere qualche notazione di carattere generale, con l'intendimento manifestato all'inizio, che è quello di cogliere i tratti salienti del diritto dell'informatica, anche nei suoi rapporti con l'informatica giuridica.

I- Intanto è possibile affermare, senza tema di smentita, che ormai esiste un corpus normativo, consistente e ben definito, di norme volte a disciplinare le relazioni tra nuove tecnologie comunicative e diritto.
Si tratta di un novero ormai notevole di disposizioni, spesso disseminate nei più svariati interventi normativi, tanto da porre al giurista problemi di coordinamento, quando non addirittura di reperimento. A questo proposito, possiamo sottolineare che vi è chi già auspica di radunare tali disposizione in un unico codice della e per la Società dell'Informazione, sulla scia di un percorso suggerito già da Frosini in relazione all'adozione di un codice mondiale per internet (peraltro di recente riecheggiato da Rodotà, il quale parla di una costituzione mondiale per l'internet), così completando il processo di codificazione per settori che sembra al momento caratterizzare tutte le aree che potremmo definire "a maggior rilevanza informatica" (codice protezione dati; statuto generale del commercio elettronico; codice amministrazione digitale; diritto d'autore società informazione)[33]. Si può ritenere quindi che, a

della legge 16 gennaio 2003, n. 3. pubbl. in GU n. 97 del 28.04.05.

[32] FROSINI, L'orizzonte giuridico dell'internet, in Dir. Inf. N. 2/2000, p. 275.

[33] FROSINI, Tante regole, troppe fonti ci vuole un codice mondiale, in Telema, Attualità e futuro della società multimediale, fondazione Bordoni, Roma 1997, 72 e ss.

differenza di quanto accadeva quando i padri nobili dell'informatica giuridica affrontavano le prime questioni poste dal computer al giurista, il panorama legislativo si sia arricchito di una mole tanto massiccia da richiedere un notevole impegno ricognitivo e interpretativo al giurista positivo.

Si tratta, per giunta, di un corpus dotato di elevata specificità, se è vero come affermato da Guido Alpa, riferendosi in particolare alla regolamentazione del commercio elettronico, che si è di fronte ad "una disciplina di settore altamente specializzata, il cui accesso appare davvero ostico"[34].

L'esistenza di questo corpus fa emergere anche che la risposta all'interrogativo posto all'inizio, se cioè le nuove modalità di svolgimento dell'attività giuridica o anche i nuovi diritti potessero essere governate esclusivamente dalle regole tradizionali è senz'altro di segno negativo.

Inoltre, abbiamo più volte rilevato che i settori di intervento del legislatore del diritto dell'informatica sono tra loro interconnessi e la disciplina del diritto dell'informatica fornisce strumenti per un approccio non più settoriale, come in passato, ma coeso, interdisciplinare e necessariamente collegato e complementare all'informatica giuridica.

La coesistenza dei due ambiti applicativi, l'uno volto verso l'informatica giuridica, avente come campi di indagine la documentazione, l'informatica giudiziaria, la legimatica, l'altro volto invece alle nuove problematiche scaturenti dallo sviluppo della Società dell'Informazione, impone per il giurista l'esigenza di dare il suo contributo per la costruzione di una società per così dire digitale, la cui definizione non può essere di esclusiva competenza dei tecnologi, ma necessariamente deve trovare collocazione e regolamentazione all'interno del sistema giuridico di riferimento, che necessita pertanto di una dignità autonoma.

II - Una seconda considerazione, appena accennata, che conferma l'impegno richiesto al giurista positivo, riguarda la complessità del sistema delle fonti del diritto dell'informatica.

Vi è un numero rilevante di norme di derivazione comunitaria (si tratta di un innegabile portato della rilevanza economica delle comunicazioni elettroniche – si pensi alla origine comunitaria delle regole sul commercio elettronico); altre sono di impulso interno, autonomo, anche in relazione alla loro finalità, chiaramente improntata allo snellimento semplificazione e trasparenza ed efficienza della P.A. anche nel rapporto con i cittadini, e si pensi, per tutte, al codice dell'amministrazione digitale (come già peraltro era avvenuto con la legge sulla firma digitale, che costituisce, per molti aspetti, l'antecedente normativo del codice dell'amministrazione digitale).

E' anche, quello dell'informatica, un diritto di formazione negoziale privata, autodisciplinare, un tipico esempio di *soft law;* basti pensare, nuovamente, alla disciplina del commercio elettronico, rispetto alla quale il legislatore comunitario, ed ora quello del recepimento, promuovono l'adozione di codici di condotta, al momento non ancora predisposti dalle categorie interessate; o anche ai codici di condotta ora previsti dall'art. 117 del codice in materia di protezione dei dati personali. Questi ultimi, peraltro, sembrano porsi sul versante più avanzato di tali modalità regolative, tanto è vero che a seguito della loro emanazione vengono "allegati" al codice e che il rispetto delle regole in essi contenute costituisce condizione di

[34] ALPA, Presentazione a TOSI (a cura di), Commercio elettronico e servizi della società dell'informazione, cit., XVI.

liceità del trattamento dei dati – sono i cosiddetti codici di condotta "di terza generazione", qualificati dallo stesso Garante "fonti normative atipiche di secondo grado"[35]. Si tratterebbe quindi, come ha affermato lo stesso Rodotà, di codici che non sono più ascrivibili alla sfera del *soft law*, e al tempo stesso non possono essere fatti ricadere semplicisticamente in quella dell'*hard law*[36].

A queste fonti, tutte ben note, se ne sta aggiungendo un'altra, le cui ricadute sulla nostra attività di interpreti e di operatori del diritto sono ancora tutte da scoprire: essa è rappresentata dalla legislazione regionale concorrente, fondata sull'attuale articolo 117 della costituzione.

Si tratta di una potestà destinata, soprattutto nella fase iniziale del suo esercizio, a porre problemi di esatta perimetrazione e di coordinamento con la legislazione primaria statale, e sono note le questioni già pervenute al vaglio della corte costituzionale in ipotesi nelle quali si è ritenuto che il legislatore regionale avesse invaso la competenza esclusiva dello Stato o avesse legiferato, nelle materie di competenza concorrente, violando i principi generali della materia demandati invece alla legge dello Stato.

A questo proposito, la riferita sentenza 271/2005 della Corte costituzionale ha chiarito entro quali limiti sussiste la possibilità, per le regioni, di legiferare in materia di coordinamento informatico dei dati, nonostante l'attribuzione esclusiva di tale materia allo Stato.

III - La terza ed ultima considerazione attiene a quell'aspetto relazionale di cui si parlava all'inizio, al rapporto ciò tra il diritto dell'informatica e l'informatica giuridica ma anche con le altre branche della scienza giuridica.

Ebbene, quello che si è appena sinteticamente disegnato è un corpus normativo complesso, che necessita, per essere correttamente ed efficientemente interpretato dal giurista che voglia avvicinarsi a quelle attività che, ormai sempre più spesso, si svolgono con modalità (e quindi anche secondo regole) informatiche e fruibile da parte del cittadino, di una elaborazione univoca di concetti e, quindi di un elevato livello di astrazione.

Tale processo sembra già in fase piuttosto avanzata, anche grazie al lavorio della dottrina e, ormai, anche della giurisprudenza. Si pensi alla già avvenuta fissazione, peraltro sempre migliorabile, di taluni concetti: pensiamo alle definizioni di banca di dati, firma digitale, firma qualificata, autenticazione informatica, indirizzo elettronico, contratto telematico, documento informatico, servizio della società dell'informazione; sono solo alcuni esempi di concetti basilari, senza la cui elaborazione non è possibile alcuna definizione, e la cui inequivoca determinazione è presupposto fondamentale della corretta comprensione e applicazione di un numero cospicuo di norme, sparse tra testi normativi differenti.

Si tratta, inoltre, di una concettualizzazione caratterizzata da un elevato tasso di "trasversalità", tale da stemperare anche le troppo rigide partizioni scolastiche (ad esempio privato/pubblico).

Il discorso sui concetti induce ad un'ultima considerazione, suggerita dalla rilettura della prefazione di Pietro Rescigno all'ultima edizione, del 2001, del I volume del Manuale di diritto dell'informatica di Ettore Giannantonio[37].

---

[35] Si veda la relazione per l'anno 2001 del Garante della privacy.

[36] RODOTA', Tra diritti fondamentali ed elasticità della normativa: il nuovo codice sulla privacy, in Europa e diritto privato, 2004, 8.

[37] RESCIGNO, Prefazione a GIANNANTONIO, Manuale di diritto dell'informatica, I, Milano, 2001, XI e ss.

Rescigno osserva che la novità del diritto dell'informatica ripropone, in chiave attuale, gli interrogativi che si sono già posti in passato rispetto al carattere autonomo di materie quali il diritto agrario o il diritto industriale, e che sono stati solitamente risolti facendo riferimento ai criteri dell'autonomia delle fonti, dell'autonomia scientifica e di quella didattica.
Ebbene, volendo applicare anche al diritto dell'informatica questo paradigma, sembra di poter dire che l'esistenza di un corpo organico di norme disciplinante le relazioni tra diritto e tecnologie dell'informazione e della comunicazione sia un dato innegabile (con la conseguenza che il primo requisito è soddisfatto); che l'autonomia scientifica, che lo stesso Rescigno qualifica come scoperta o ricognizione di un apparato concettuale proprio, è pure senz'altro presente, quantunque non ancora pervenuta ad un soddisfacente livello di consolidazione, e si tratta di un'autonomia costruita intorno all'elemento unificante e trasversale della comunicazione elettronica; quanto al terzo elemento, che Rescigno individua nel fatto che l'insegnamento di una materia venga impartito nell'ambito dei corsi di laurea, sappiamo bene che pure è di fatto sussistente. Si pensi, per esempio, all'attivazione, in questi ultimi anni, di molti corsi aventi oggetto la materia che qui ci interessa, seppur sotto diverse denominazioni (diritto dell'internet, diritto delle nuove tecnologie, etc., oltre agli insegnamenti tradizionali di informatica giuridica), attraverso i quali si è inteso sottolineare la necessità e l'importanza dello studio di queste tematiche per la formazione del giurista della cosiddetta Società dell'Informazione.
Una ulteriore conferma della rilevanza e del carattere autonomo del diritto dell'informatica sembra desumersi dal decreto 25 novembre 2005 del Ministero dell'Istruzione dell'Università e della Ricerca (pubblicato sulla G.U. del 17 dicembre 2005), avente ad oggetto la revisione della classe delle lauree magistrali in Giurisprudenza, il cui allegato, nell'ambito dei così definiti "obiettivi formativi qualificanti", precisa come uno degli sbocchi di elezione dei laureati dei nuovi corsi di tale classe riguardi proprio il "settore del diritto dell'informatica", nel quadro di un corso di studi che tende a potenziare anche la capacità di produrre testi giuridici (normativi, negoziali e processuali) e ad assicurare l'acquisizione di adeguate conoscenze di informatica giuridica.

Postilla

Una riflessione di carattere filosofico sul fondamento del diritto dell'informatica

Lo studio del fenomeno dell'informatica giuridica e del diritto dell'informatica può sollecitare anche riflessioni di carattere filosofico, rispetto alla cognizione del fondamento logico.
Assumendo quindi una prospettiva filosofica, l'essenza del sistema è nella contraddittorietà: ordine e disordine, diritto e negazione del diritto. Questa stessa chiave di lettura, applicata al diritto dell'informatica ci fa vedere come l'ordinamento abbia attraversato una fase di disordine, determinata dalla novità del fenomeno, seguita poi da una fase di osservazione da parte del giurista, che ha cercato le risposte nella normativa già esistente, ed infine da una fase, se così si può dire, appena iniziata di vera e propria codificazione.

Rispetto alla fenomenologia della rete internet esiste un fondamento univoco sulla questione della sua regolamentazione?
Ogni fenomeno scientifico, culturale e sociale spesso necessita di prevedibilità, di coordinazione, di ciò che in termini filosofici si individua in un fondamento. Il problema che conseguentemente ci si pone è se l'esigenza di tale fondamento, di ciò che qualcuno definisce "dominio incontrastato di un centro", possa coesistere nel peculiare mondo della rete nell'ambito di una società sempre più digitalizzata.
Se si parte dal presupposto per cui attraverso la comunicazione elettronica si realizza una reciprocità di comunicazioni, dove chi è fornitore di una informazione può essere al contempo destinatario di informazioni da altri trasmesse, si capisce anche che questa stessa corrispettività di comunicazioni esclude l'idea di un centro intorno a cui si possa muovere "un'immensa periferia".
In questa prospettiva e traendo spunto dalle teorie filosofiche post-moderne in cui si evidenzia il principio della dissoluzione del modello c.d. centrale, può risultare legittima la domanda se davvero la ormai acclarata realtà digitale abbia bisogno di un centro, di un fondamento filosofico (si pensi all'io categorico Kantiano o alla norma fondante di Kelsen), che costituisce il presupposto di tutto il procedimento normativo, come fondamento giusfilosofico.
La risposta, oggi, secondo l'evoluzione della rete, è che la rete stessa è divenuta il centro attorno al quale gravitano una molteplicità di periferie.
La regolamentazione allora riguarda i fenomeni agganciabili all'evolversi della tecnologia, e quindi alla società digitale, ma non alla rete direttamente, come fattore neutrale: l'intervento avviene necessariamente in modo trasversale, proprio perché la tecnologia evidenzia le divergenze e convergenze dei diversi fenomeni esistenti nella dinamica dell'ordinamento giuridico.
In questo percorso evolutivo si potranno cercare, anche in ambito filosofico, le ragioni teoretiche per una positiva valutazione delle possibilità che le tecnologie dell'informazione e della comunicazione e con essa lo sviluppo della società digitalizzata offrono, non solo, per un ripensamento dell'esistenza di nuove materia a cui riconoscere autonomia scientifica, normativa, didattica, ma anche al fine di inquadrare l'essenza stessa del pensiero fuori dai canoni ereditati dalla modernità.

Rivista elettronica di Diritto, Economia, Management

N. 1 - 2010 • pp. 89-115

Teoria e pratica nell'interpretazione del reato informatico

Paolo Galdieri

Abstract: L'impiego delle tecnologie dell'informazione in tutti i settori della vita sociale ha comportato quale "rovescio della medaglia" il proliferare di condotte lesive degli interessi individuali e collettivi. Il fenomeno della criminalità informatica è finito sotto la lente di ingrandimento dei legislatori di tutti i Paesi dell'Unione europea e di molti altri che hanno quindi adottato normative *ad hoc*. L'Italia in ossequio alle indicazioni comunitarie, seppur in ritardo, si è dotata di una legislazione ampia ed articolata, in grado di realizzare un aggiornamento sia del codice penale, che di quello processuale. Scopo del presente articolo è, quindi, quello di verificare come l'attuale assetto normativo sia stato recepito nel nostro Paese, cercando di individuare quanti e quali siano i problemi ancora aperti. A tal fine verranno individuate le disposizioni di legge, i relativi contenuti ed i contesti cui le stesse sono chiamate ad operare anche per comprendere come ciascuno di tali elementi possa rilevare nelle diverse fasi del procedimento penale ovvero in quella delle indagini preliminari e dell'eventuale successivo giudizio.

Parole chiave: tecnologie dell'informazione, criminalità informatica, reato transnazionale, reato a distanza, anonimato, Convenzione di Budapest, hacker

Articolo pervenuto il 7 ottobre 2010, approvato il 24 novembre 2010

1. Informatica e diritto: punti di interazione

Il diritto, in quanto scienza sociale, non può restare indifferente innanzi agli effetti prodotti dall'impiego delle tecnologie dell'informazione all'interno della società civile. L'introduzione degli elaboratori negli uffici privati, pubblici e, da alcuni anni grazie alla diffusione dei *personal computers*, nelle abitazioni, ha radicalmente mutato il modo di lavorare, di agire e, per alcuni versi, di pensare. L'opportunità di acquistare a distanza beni di ogni tipo, conseguente alla trasformazione della moneta cartacea nella cosiddetta moneta elettronica, di dialogare in rete con soggetti collegati da parti opposte del mondo, sono solo alcuni esempi di ciò che è possibile realizzare attraverso le metodologie informatiche.

Inevitabilmente questi fenomeni sono finiti sotto la lente di ingrandimento del giurista, che ha cominciato a comprendere l'importanza delle nuove tecnologie anche rispetto ai settori che riguardano le materie di sua pertinenza.[1]

La possibilità di trattamento automatico dell'informazione giuridica ha iniziato a realizzarsi per i giuristi e gli operatori del diritto più di quaranta anni fa e si è concretizzata inizialmente in due linee di sviluppo: 1) l'automazione dei sistemi di documentazione giuridica, concernente la generazione, la gestione e la ricerca di informazioni in archivi elettronici e banche di dati; 2) la regolamentazione giuridica delle conseguenze delle applicazioni dei sistemi di elaborazione dei dati sulla società.

All'inizio degli anni '70, con l'evolversi ed il diffondersi della tecnologia informatica, si è sviluppata l'informatica giuridica di gestione, riguardante l'automazione del processo di formazione dei documenti e degli atti giuridici e, in tempi più recenti, del processo di formazione della stessa decisione giuridica.

Contemporaneamente lo studio della regolamentazione giuridica degli strumenti e delle attività informatiche si è venuto sempre più staccando dalle problematiche tecniche, alle quali era alle origini legato, fino a configurarsi come diritto dell'informatica.

Gli ultimi anni sono caratterizzati dalla diffusione di massa dei *personal computers* in tutte le attività degli operatori del diritto, da alcune applicazioni di intelligenza artificiale a problemi giuridici, e da uno sviluppo della telematica come veicolo per la distribuzione di informazione e di atti giuridici.

Dunque, usando la terminologia odierna, l'interazione tra informatica e diritto si è evoluta secondo due linee principali: l'informatica giuridica e diritto dell'informatica. Indicando con la locuzione generale di "informatica giuridica" [2] tutte le situazioni ove si determina un'interazione tra informatica e diritto, mentre con la formula "diritto dell'informatica" il complesso di norme che disciplinano l'uso delle tecnologie informatiche.

Le indagini teoriche degli studiosi hanno seguito l'evoluzione descritta, anche se ciascuno, nell'inquadrare l'informatica giuridica, ha privilegiato la linea o le linee più conformi alla propria formazione intellettuale e più vicine al proprio settore operativo. Non a caso i giuristi

---

[1] Cfr.: V. Frosini, *Il diritto nella società tecnologica*, Giuffrè, Milano, 1981, P. 249 ss.; ID., *Informatica, diritto e società*, Giuffrè, Milano, 1992, 2° ed. ampl., p. 119 ss.

[2] V. Frosini, *Informatica, diritto e società*, op. cit., p. 339 ss.

che si sono dedicati in Italia all'informatica giuridica si sono soffermati soprattutto sul diritto dell'informatica, in modo quasi esclusivo nei primi anni e prevalente ancora oggi.
Le posizioni scaturenti dalle varie indagini non sono quindi classificabili in categorie fisse, anche se spesso, per dare una veste sistematica a un rapporto fra informatica e diritto si possono individuare tre temi ricorrenti di discussione: il rapporto fra informatica e diritto nell'informatica giuridica, la definizione del contenuto della disciplina, e l'autonomia di quest'ultima nei confronti di altre discipline giuridiche come la filosofia del diritto, la teoria generale del diritto o la sociologia giuridica.

2. Il diritto dell'informatica

L'utilizzazione dei beni e dei servizi informatici è regolata attraverso un complesso di norme giuridiche il cui insieme viene indicato generalmente attraverso la locuzione "diritto dell'informatica".
Tuttavia, se la disciplina riguardante i contratti informatici, le responsabilità del gestore di un sistema o la costituzione di una banca dati può essere ricavata dall'ordinamento civile, la protezione di determinati beni messi in pericolo da alcune condotte non autorizzate (pensiamo alle intrusioni informatiche o alla frode perpetrata attraverso il computer), viene accordata da disposizioni facenti capo al diritto penale, così come anche altri rapporti correlati all'informatica trovano la loro qualificazione all'interno di norme appartenenti al diritto amministrativo.
Pare pertanto evidente che le norme informatiche si caratterizzano per la loro natura ancipite. Da un lato, esse si assomigliano per il fatto di prevedere un aspetto informatico; dall'altro, si differenziano per l'appartenenza ad una branca specifica dell'ordinamento giuridico (penale, civile, amministrativa, ecc.).
Ben presto si è posto il problema di comprendere se il diritto dell'informatica costituisca una branca autonoma dell'ordinamento o piuttosto una semplice formula descrittiva in grado di raccogliere disposizioni aventi natura e miranti a perseguire finalità differenti.
Nell'ambito degli informatici era diffusa l'idea che non fosse necessario predisporre normative ad *hoc* in quanto tra gli operatori del settore si era ormai instaurata una prassi consolidata che consentiva di risolvere diverse questioni. Altro argomento è che le problematiche poste dall'informatica variano di continuo e quindi ogni norma sarebbe destinata in breve tempo a perdere valore.
Negli ambienti giuridici, invece, non si contestava tanto l'esigenza di norme specifiche, che nel tempo sono state emanate, quanto che le stesse formassero nel loro insieme un diritto ed una scienza giuridica nuovi ed autonomi rispetto alle tradizionali partizioni del sistema. Tale convincimento prendeva le mosse dalla considerazione che l'autonomia di una scienza richiede l'omogeneità delle materie in essa comprese ed un tratto comune che le distingua dalle altre scienze o rami del diritto. Tutto ciò verrebbe a mancare nel nostro caso in quanto, come sopra detto, le norme in parola sono caratterizzate solo sotto il profilo meramente contenutistico, perché tutte si riferiscono all'informatica, ma per il resto perseguono obiettivi eterogenei e sono ciascuna riconducibile all'interno di settori già esistenti dell'ordinamento giuridico.

Di contro, secondo autorevole dottrina [3], l'applicazione degli istituti tradizionali nel campo dell'informatica, argomento forte dei giuristi che negano un'autonomia del diritto dell'informatica, non è sempre agevole e, talvolta, dà risultati non soddisfacenti. Tali difficoltà si incontrano quando si tenta di ricondurre i programmi informatici nell'ambito delle opere dell'ingegno, così come anche quando si cerca di ricondurre taluni fatti all'interno delle norme penali previgenti.
Ciascun ostacolo trova la sua scaturigine nel *computer* che è, infatti, una macchina diversa da tutte le altre, capace cioè di distinguere e di connettere dati e di reagire al verificarsi di predeterminate situazioni.
Sempre ad avviso di tale dottrina l'introduzione dell'informatica nella vita sociale comporterebbe la configurazione di un nuovo tipo di bene, l'attività automatica, che non è possibile inquadrare nella tradizionale distinzione dei beni giuridici e degli oggetti di diritto [4].
La natura dell'attività automatica costituirebbe, quindi, la ragione della particolarità del diritto dell'informatica e ciò che ne delimiterebbe i confini.
Se superate paiono le obiezioni riguardo alla necessità di regolamentare l'uso delle tecnologie informatiche, così come è acquisita la consapevolezza della specificità dei beni informatici, ciò nonostante è da ritenere che il diritto dell'informatica non possa essere, comunque, considerato quale nuovo ramo del diritto. A ben vedere, infatti, la natura peculiare dei beni informatici, pur imponendo una ridefinizione di istituti tradizionali e una concettualizzazione di problemi nuovi, non può portare ad una unificazione di fatti che, per gli obiettivi perseguiti ed i contesti in cui si realizzano, finiscono inevitabilmente con l'essere assorbiti all'interno delle partizioni del sistema giuridico già esistenti.

3. La percezione della criminalità informatica in Italia

Sino a poco tempo fa, in Italia, i reati informatici non erano considerati come una concreta minaccia per la società e ciò per un diverso ordine di ragioni.
A contenere il timore della commissione di reati informatici contribuiva in primo luogo la modalità di utilizzo del *computer*. In tempi non così lontani, infatti, solo in pochi, principalmente imprese ed enti pubblici, erano dotati di sistemi informatici e comunque anche laddove gli stessi venivano utilizzati non erano accessibili dall'esterno, costituendo tra loro al massimo delle reti chiuse. Tale situazione impediva di fatto la commissione del reato informatico, nelle ipotesi di assenza di computer, o la limitava al massimo, nel senso che nel caso di reti chiuse era ipotizzabile esclusivamente la commissione del reato da parte di soggetti che operavano all'interno della struttura ove si trovavano. Conseguenza di ciò era che non potevano realizzarsi reati telematici, per es. accessi nel sistema dell'impresa da luogo diverso da quello dove lo stesso si trovava, e in caso di commissione di illecito sarebbe stato relativamente agevole individuarne l'autore, visto che l'indagine si sarebbe limitata alle persone che fisicamente

[3] E. Giannantonio, *Manuale di diritto dell'informatica*, Cedam, Padova, 1994, p.3.

[4] E. Giannantonio, *Manuale di diritto dell'informatica*, op. cit., p.6.

avevano diritto di accesso ai locali dove il sistema era collocato.
Altra ragione che influiva sul negare rilevanza al reato informatico era quella che in una prima fase i *computers*, anche quelli delle imprese, contenevano informazioni di scarso valore, essendo utilizzati per svolgere singole attività di tipo quasi esclusivamente burocratico. Entrare all'interno del sistema non costituiva quindi serio "affare" per il malintenzionato, atteso che avrebbe carpito o distrutto informazioni di scarso valore economico e strategico, ed al contempo, proprio la natura dell'informazione contenuta nel sistema, non avrebbe determinato grosse perdite per il titolare del sistema informatico attaccato.
A "snobbare" il reato informatico contribuiva, infine, una scarsa conoscenza del fenomeno, che portava a considerare i delitti informatici frutto di azioni "isolate" e quindi prive di rilevanza.
Ben presto, tuttavia, ci si accorse che le scarse informazioni sulla criminalità informatica, specie quella rivolta contro le aziende, non dipendevano tanto e solo dalla evanescenza della stessa quanto dalla ritrosia della vittima del reato a denunciare l'attacco subito. Nella maggior parte dei casi, specie le aziende, pur avendo subito un attacco informatico decidevano di non denunciarlo temendo che tale denuncia avrebbe comportato una pubblicità negativa e quindi un nocumento maggiore di quello subito, pubblicizzando di fatto una scarsa tutela dei sistemi da parte del denunciante. A scoraggiare le vittime di tali reati a sporgere querela vi era poi l'idea diffusa che l'azione penale non avrebbe portato alcuna conseguenza positiva, poiché, mancando previsioni penali specificatamente riferite alla criminalità informatica, il procedimento aperto si sarebbe concluso con grande probabilità con un'archiviazione o al massimo con un'assoluzione del soggetto individuato come autore della condotta illecita.
Nel volgere di pochi anni, tuttavia, la situazione è radicalmente mutata e diverso risulta essere l'atteggiamento rispetto a tale tema.
Alla base di tale inversione di rotta si colloca in primo luogo il diverso utilizzo del *computer*. Oggigiorno la maggior parte dei soggetti è dotata di diversi *computers* e gli stessi sono sovente accessibili dall'esterno, costituendo delle reti aperte. La presenza capillare dei *computers* fa si che in astratto in qualunque impresa, ad esempio, possa essere commesso un reato informatico; l'accessibilità dall'esterno rende possibile attacchi da soggetti che non fanno parte dell'organico aziendale e quindi una maggiore difficoltà nella loro individuazione. Colui che decide di commettere un reato di questo tipo, potendolo realizzare a distanza, ha maggiore probabilità di non essere rintracciato.
Vi è poi da considerare che attualmente il patrimonio dell'azienda è totalmente dematerializzato, nel senso che all'interno del *computer* vengono inserite tutte le informazioni relative all'attività dell'impresa, sia di contenuto economico, che strategico. L'accesso ad un *computer* aziendale risulta quindi vantaggioso per il "delinquente informatico", poiché la condotta posta in essere può portare ingenti guadagni per lui ed, al contempo, determinare ingenti danni all'impresa colpita.
Sotto tale ultimo aspetto rileva come la commissione di un reato informatico all'interno di un'azienda determini un triplice danno per la stessa e segnatamente: un costo per riattivare o sostituire le risorse informatiche colpite; un nocumento, non sempre agevolmente stimabile, riguardante direttamente la diminuzione del patrimonio aziendale riconducibile all'attacco informatico; un danno, altrettanto difficile da quantificare, relativo all'immagine dell'impresa colpita.

Anche sul piano giuridico si registrano importanti mutamenti visto che nel volgere di pochi anni sono state previste dal legislatore diverse ipotesi di reato informatico, la maggior parte delle quali introdotte dalla legge 547 del 93. Ne consegue che se oggi si decidesse di denunciare il delitto subito, si potrebbe quanto meno contare sull'effettiva possibilità di ottenere soddisfazione all'interno del processo penale instaurato.

4. Il Diritto penale dell'informatica

L'interdisciplinarietà dell'informatica giuridica e del diritto dell'informatica determina l'esigenza di verificare l'esatta portata di qualsiasi problema, posto in linea generale da ciascuna delle discipline, riconducendolo all'interno dello specifico settore dell'ordinamento considerato.
Così come l'informatica giudiziaria, il discorso vale anche per le altre sottocategorie del'informatica giuridica, pone questioni differenti a seconda che il computer venga inserito nelle dinamiche del processo civile, penale o amministrativo, differenti essendo le regole che lo muovono, così anche la norma informatica, dalla sua emanazione alla sua applicazione, presenta problematiche proprie dell'ordinamento (civile, penale, amministrativo, ecc.) cui appartiene.
L'assunto non tende, in vero, a giustificare la nascita di un'informatica giuridica civile, penale e amministrativa e parallelamente, il sorgere di diversi nuovi diritti (penale, civile ed amministrativo, ecc.) dell'informatica; ciò che si vuole invece sottolineare, è che compresa l'essenza dell'informatica i problemi di interesse giuridico dalla stessa posti vanno valutati all'interno di un preciso contesto di riferimento e passati al vaglio delle regole che lo sottendono.
Anche rispetto all'ordinamento penale è possibile distinguere due aree "di interferenza informatica". La prima è quella che si riferisce alle situazioni in qualche modo collegate all'accertamento di un fatto costituente reato o comunque riconducibili ad attività di supporto per la realizzazione dei suddetti obiettivi. Vengono, quindi, prese in considerazione le applicazioni informatiche che agevolano gli organi di polizia ed il pubblico ministero nella fase delle indagini preliminari, che favoriscono la comprensione del fatto, contribuendo a determinare il convincimento dei giudici nella fase dell'emanazione della sentenza, che svolgono un ruolo fondamentale nell'attività degli avvocati e della dottrina, specie riguardo al reperimento delle fonti.
Altra area di interferenza è quella caratterizzata dall'accorpamento delle norme che consentono di realizzare la tutela penale dell'informatica o meglio dei soggetti che ne fanno uso, il cui insieme viene indicato come Diritto penale dell'informatica.
Queste norme si distinguerebbero, in vero, per la loro natura ancipite. Da un lato, in quanto riferite a fatti informatici, pongono questioni giuridiche che derivano direttamente dalla loro connotazione tecnologica e sono, quindi, assimilabili alle norme del diritto dell'informatica, che gravitano nell'orbita delle altre branche dell'ordinamento giuridico (civile, amministrativo, ecc.); dall'altro, in quanto volte a perseguire interessi ben individuati, sono accostabili a tutte le altre disposizioni del diritto penale che pur non si riferiscono a fatti informatici.
D'altra parte, se questi sono i rapporti che intercorrono tra le norme penali informatiche e le

norme informatiche non penali e tra le prime e le norme penali non informatiche, ulteriori distinguo si possono fare all'interno della categoria delle norme penali informatiche.
Le norme penali informatiche possono dividersi in tre gruppi fondamentali: 1) norme penali eventualmente informatiche; 2) norme penali informatiche in senso ampio; 3) norme penali informatiche strictu sensu. Norme penali eventualmente informatiche sono tutte quelle disposizioni che, non prevedendo una specifica modalità di condotta, bensì esclusivamente un determinato evento, disposizioni cosiddette a forma libera, possono, al determinarsi di certe condizioni, essere applicate anche a fatti realizzati contro, o per mezzo, le tecnologie dell'informazione. Per tutti si prenda l'esempio del reato di estorsione (art. 629 c.p.), che può realizzarsi anche minacciando di lasciar inserito un virus informatico, abusivamente introdotto dentro il sistema, se non verrà pagata una determinata somma entro un certo termine.
Norme penali informatiche in senso ampio sono invece tutte quelle disposizioni che, pur riferendosi espressamente ed esclusivamente a fatti informatici, costituiscono un semplice aggiornamento in chiave tecnologica di norme preesistenti. Pensiamo all'esercizio arbitrario delle proprie ragioni (art. 392 c.p.) che, grazie alla modifica apportata dalla l. 547/93, può riferirsi oltre che alla violenza su una cosa mobile anche a quella realizzata contro un bene informatico.
Vi sono, infine, disposizioni espressamente ed esclusivamente riferite a fatti informatici che, considerando situazioni completamente nuove rispetto al passato, comportano valutazioni diverse da quelle comunemente adottate, norme penali informatiche strictu sensu. E' questo il caso dell'art. 615-ter (introdotto dall'art. 4 l. 547/91), che consente di punire l'accesso non autorizzato all'interno del sistema informatico.
Altra distinzione possibile è quella che fa leva sul ruolo giocato dall'informatica nella dinamica del reato. Volendo restringere al massimo le ipotesi possibili si individuano due categorie fondamentali. La prima riunisce tutti i fatti in cui l'informatica costituisce l'oggetto su cui ricade l'azione prevista e punita dall'ordinamento penale. Rientrano in questa categoria il reato di danneggiamento informatico, il falso informatico, ecc. La seconda categoria raccoglie invece tutti i fatti in cui l'informatica costituisce il mezzo per perseguire un risultato previsto e punito dall'ordinamento penale. Appartengono a questo raggruppamento la frode informatica, e molti delitti eventualmente informatici (estorsione perpetrata a mezzo di virus, omicidio commesso attraverso computer, ecc.). A questi fatti vanno poi aggiunti altri (es.: l'ipotesi base dell'accesso non autorizzato in un sistema informatico o telematico) in cui l'informatica è contemporaneamente oggetto e mezzo dell'attività delittuosa, e che quindi, a differenza degli altri reati parzialmente informatici, possono definirsi reati totalmente informatici.
Prescindendo dalle succitate distinzioni è comunque innegabile che, rispetto alle altre disposizioni penali, quelle a contenuto informatico introducono questioni giuridiche peculiari.[5]. I problemi del diritto dell'informatica diventano in quest'ambito il problema

5 Tra le diverse monografie aventi ad oggetto la criminalità informatica si segnalano: R. Borruso, G. Buonomo, G. Corasaniti, G. D'Aietti, *Profili penali dell'informatica*, Giuffrè, Milano 1994; F. Buffa, *Internet e criminalità*, Giuffrè, Milano, 2001; G. Ceccacci, *Computer crimes*, FAG, Milano, 1994; P. Galdieri, *Teoria e pratica nell'interpretazione del reato informatico,* Giuffrè, Milano, 1997; G. Pica, *Diritto penale delle tecnologie informatiche*, UTET, Torino, 1999; G. Pomante, *Internet e criminalità*, Giappichelli, Torino, 1999; C. Sarzana, *Informatica e diritto penale*, Giuffrè, Milano, 1994.

dell'individuazione del bene, o dei beni, giuridici meritevoli di tutela; il problema dell'eventuale equiparazione cose mobili - programmi, dati ed informazioni; il problema di conferire valore alla presenza di un nuovo soggetto nelle dinamiche del reato: il computer.

5. Prospettazioni teoriche ed opzioni normative

Sebbene l'emanazione delle norme penali informatiche si sia realizzata nei diversi Paesi in tempi e con modalità talvolta differenti, ciononostante è possibile tracciare per vie generali il percorso che ha condotto verso una legislazione penale dell'informatica.
Quando le tecnologie dell'informazione erano utilizzate solo in particolari contesti, quali ad es. i grandi complessi aziendali o i settori pubblici di interesse strategico (militare, ricerca, ecc.) e ancora se ne ignoravano le reali potenzialità, alcuni lungimiranti studiosi iniziarono a porsi il problema della regolamentazione giuridica delle nuove tecnologie.
È abbastanza singolare, seppure vi sia una ragione logica, che in questa fase apporto fondamentale venga dai filosofi del diritto, e non piuttosto dai civilisti e dai penalisti, direttamente interessati dai nuovi fenomeni. La ragione di ciò risiedeva nel fatto che in assenza di una casistica degna di rilievo e di norme, e dovendosi di conseguenza muovere su un piano prevalentemente astratto, coloro che provenivano da studi filosofici avevano un approccio più adatto a comprendere la situazione. In questo periodo le questioni di maggiore interesse erano quelle della tutela della riservatezza da intromissioni via *computer* e quelle del'individuazione di nuovi beni giuridici direttamente prodotti dall'informatica.
Ben presto l'introduzione dei *personal computers,* e la conseguente crescente alfabetizzazione informatica, allargarono la cerchia dei soggetti in grado di utilizzare il *computer* ed al contempo favorirono il sorgere di un certo tipo di criminalità informatica.
La situazione veniva avvertita anche dai cultori del diritto positivo che nel sollecitare l'intervento legislativo proponevano due soluzioni alternative[6]. Secondo un orientamento assai diffuso in Europa i nuovi delitti non introducevano interessi meritevoli di tutela, bensì producevano soltanto nuove modalità di aggressione di beni giuridici preesistenti. Quest'orientamento portava a sostenere il cosiddetto metodo evolutivo e cioè la necessità di introdurre singole disposizioni specificatamente riferite all'informatica all'interno delle normative penali previgenti.
Per altro indirizzo dottrinario, sviluppatosi per lo più nei Paesi anglosassoni, le nuove tecnologie determinavano il sorgere di nuovi interessi suscettibili di protezione e quindi era auspicabile un intervento specifico ed autonomo in grado di disciplinare separatamente dalle normative previgenti l'intero fenomeno criminale (metodo della c.d. legge organica).
Anche gli organismi sovranazionali si posero il problema di indirizzare i singoli Paesi attraverso iniziative di vario genere. La Cee, ad esempio, attraverso un comitato ristretto di esperti, creato all'interno del Comitato per i problemi criminali del Consiglio d'Europa, formulò una lista dettagliata dei reati informatici. La lista, che si tradusse nella raccomandazione n.89/9,

[6] V.Frosini, *Contributi ad un diritto dell'i*nformazione, Liguori, Napoli, 1999, p.165 ss..

distingueva tra interventi normativi a tutela di ipotesi particolarmente diffuse, e che quindi dovevano essere attuati da tutti gli Stati membri, ed interventi rimessi alla discrezionalità di ciascun Paese. Gli interventi urgenti, costituenti la cosiddetta lista minima, riguardavano i seguenti atti: frode informatica, falso informatico, danneggiamento dei dati e dei programmi informatici, sabotaggio informatico, accesso non autorizzato, riproduzione non autorizzata di un programma informatico protetto, riproduzione non autorizzata di una topografia informatica. Veniva rimessa alla discrezionalità di ciascun Stato, lista facoltativa, invece, la previsione di norme relative: all'alterazione dei dati o dei programmi informatici, allo spionaggio informatico, all'utilizzazione non autorizzata di un programma informatico protetto.

Sempre in questa fase si registrò un attivo apporto della giurisprudenza che, in assenza di norme, tentò, talvolta in modo forzato, di colmare le lacune esistenti.

Pian piano comunque in tutto il mondo vennero introdotte norme penali informatiche e ciò seguendo criteri diversi.

Oltre alla scelta di fondo già citata, legge organica o metodo evolutivo, si riscontrarono altre differenze dovute sia al livello di automazione raggiunto nel singolo Paese e sia in rapporto al tipo di regime giuridico esistente, a secondo cioè che fosse di *civil* o *common law*.[7]

Negli Usa, dove si è adottato il metodo della legge organica, attraverso il *Counterfeit Access Device and Computer Fraud and Abuse Act* del 1984, modificato successivamente dal *Computer Fraud and Abuse* del 1986, furono formulate ipotesi di reato ben precise ed adatte ad arginare i fenomeni esistenti in quella realtà.

In Australia (legge del 1989 che modifica il *Crimes Act* del 1914) l'inserimento delle "infrazioni relative agli elaboratori" concerne il solo settore federale. Sono previste e punite le ipotesi di accesso illegale ai dati contenuti negli elaboratori dei servizi federali e l'alterazione dei dati contenuti negli elaboratori dei servizi federali effettuato mediante attrezzature in possesso del Commonwealth.

Tra i Paesi asiatici quello che per ovvi motivi si è attivamente interessato al problema della repressione della criminalità informatica è il Giappone che attraverso la l. n. 52 del 1987 ha previsto e punito le ipotesi di danneggiamento e sabotaggio di elaboratori commerciali altrui e le interferenze in un *computer* per il perseguimento di fini fraudolenti.

In Europa, ancor prima che fossero promulgate leggi da parte del Lussemburgo, Svizzera, Portogallo ed Italia, la legislazione penale dell'informatica aveva già preso piede. La Danimarca, con la l. n. 229 del 6 giugno 1985, aveva modificato gli artt. 193, 263 e 279a del suo codice penale, prevedendo le ipotesi dell'impedimento al buon funzionamento degli elaboratori, dell'accesso illegale ad informazioni o a programmi informatici altrui e della truffa informatica.

Verso la medesima direzione si erano mosse nel 1986 la Germania, che aveva adottato una normativa, contenuta in una sezione della seconda legge per la lotta alla criminalità economica e la Svezia, che aveva introdotto alcune modifiche del sistema penale allo scopo di assicurare una protezione contro atti rientranti nell'ambito della criminalità informatica. Nuove norme vennero emanate anche in Norvegia, attraverso l'Act n. 54 del 12 luglio 1987, ed in Austria,

---

[7] Per una visione generale delle legislazioni estere cfr: V.Frosini, *Contributi ad un diritto dell'i*nformazione, op.cit, p.165 ss.; C.Sarazana, *Informatica e Diritto penale, op.cit,* p.127 ss..

con la l. n. 695 del 1987.
Meritano di essere menzionate, inoltre, la legge francese n. 88.19 del 5 maggio 1988 (che ha introdotto il nuovo capo III del titolo II del libro III del codice penale, intitolato "Alcune infrazioni in materia informatica"), la legge greca n. 1800 del 1988 e la legge Finlandese del 1990.
Oltre alla legge Israeliana, deve ricordarsi la legge inglese, Computer Misure Act del 1990, che prevede l'accesso non autorizzato puro e semplice al materiale informatico e quello finalizzato alla commissione, o agevolazione, di un ulteriore reato, nonché la modifica non autorizzata del "contenuto" di un elaboratore.
Anche gli Emirati Arabi Uniti ultimamente, attraverso la legge federale n.2 del 2006, hanno adottato una normativa articolata in tema di crimini informatici.

6. La legislazione italiana

La legislazione italiana in materia di reati informatici può essere rappresentata come un mosaico le cui tessere sono state inserite in un lasso di tempo relativamente lungo.
Da principio, infatti, poche erano le norme riferibili, in via eventuale e non specifica, a fatti informatici, pensiamo alle disposizioni che vietano la schedatura dei lavoratori ed il controllo a distanza (artt. 4 e 8 dello Statuto dei lavoratori, l. 20 maggio 1970, n. 300) e ad alcune disposizioni del codice penale, quali ad esempio quelle riferite alla violazione dei segreti e l'art. 420 c.p., riguardante il danneggiamento degli impianti di pubblica utilità.
Nel volgere di alcuni anni si registrano però singoli interventi che, pur non colmando le lacune presenti nell'ordinamento, testimoniano un crescente interesse verso le nuove problematiche. In quest'ottica devono essere lette: la legge posta a tutela delle topografie dei prodotti a semiconduttore (l. 21 febbraio 1989, n. 70); l'art. 12 l. 1 aprile 1981 n. 121, contenente una fattispecie propria di uso illegittimo di dati e informazioni (ipotesi di abuso della privacy); l'art. 2, comma 7, l. 26 gennaio 1983, in tema di manomissione, e alterazione degli apparecchi misuratori fiscali, concernente una fattispecie che pare riguardare l'alterazione del dato di rilievo fiscale contenuto nello strumento elettronico; l'art. 12 del d.l. 3 maggio 1991 n. 143 (convertito con modificazioni con l. 5 luglio 1191, n. 197), riferito all'uso indebito di carta di credito, di pagamento e documenti che abilitano al prelievo di denaro contante.
Si giunge così dopo un annoso dibattito giurisprudenziale e dottrinario alla realizzazione di un intervento completo in ambito informatico per mezzo del d.lgs. 518/92, successivamente modificato dalla l. 18 agosto 2000 n. 248, che nell'equiparare i programmi informatici alle opere letterarie prevede anche specifiche ipotesi di reato, e soprattutto attraverso la l. 547/93, i cui contenuti sono stati successivamente ampliati attraverso la l. 18 marzo 2008 n. 48, che introduce diversi delitti.
Grazie alla legge 547 vengono riconosciuti, finalmente, sotto il profilo formale e sostanziale, i reati caratterizzati dall'elemento informatico e si determina una svolta importante nel nostro ordinamento, con riflessi evidenti in settori fondamentali quali quello dell'organizzazione della pubblica amministrazione e nel sistema fiscale. Tredici articoli (tre dei quali riguardanti la procedura penale) ridisegnano la mappa degli interessi meritevoli di tutela, introducendo

nuove ipotesi di reato ed ampliando la portata di quelle già previste.
L'opera del legislatore si muove all'interno di tutto il *corpus juris* penale interessato dal fenomeno informatico, ad eccezione dell'ipotesi del cosiddetto furto di dati. Quest'ultima non viene, infatti, contemplata da un'autonoma norma incriminatrice, in quanto si è ritenuto che "la sottrazione di dati, quando non si estenda ai supporti materiali su cui i dati sono impressi (nel qual caso si configura con evidenza il reato di furto), altro non è che una presa di conoscenza di notizie, ossia un fatto intellettivo rientrante, se del caso, nelle previsioni concernenti la violazione dei segreti. Ciò, ovviamente, a parte la punibilità ad altro titolo delle condotte strumentali, quali ad esempio, quelle di violazione di domicilio (art.614 c.p.), ecc >>[8].
Uno sguardo d'insieme consente di cogliere alcune scelte di campo ben precise. La preferenza accordata dal legislatore alla tutela penale, piuttosto che a quella amministrativa, auspicata limitatamente ad alcune ipotesi da parte di alcuni, trova giustificazione nell'esigenza di rispettare le indicazioni contenute nella circolare della Presidenza del Consiglio 19 dicembre 1983 (che prospettano l'intervento penale sulla base dell'interesse da tutelare e sul grado dell'offesa, principio di proporzione, nonché sull'inevitabilità della sanzione penale, quale ultima ratio, principio di sussidiarietà.)[9].
Verso tale direzione ci si è mossi anche per agevolare la cooperazione internazionale. Si è notato a proposito che, essendosi numerosi Stati europei ed extraeuropei dati una specifica legislazione in materia penale, ed essendo di regola richiesta la cosiddetta doppia incriminazione – ai fini dell'estradizione e di altre forme di collaborazione giudiziaria penale – l'assenza di norme penali avrebbe impedito allo Stato italiano di collaborare con gli altri Stati nella lotta contro la criminalità informatica. C'era poi l'esigenza di adeguare la legislazione italiana alle direttive impartite da organismi sovranazionali ai quali l'Italia aderisce[10].
In linea con il più ampio disegno di politica penale volto ad arginare il fenomeno della decodificazione, si è optato per una modifica del codice penale piuttosto che per una legge penale speciale; nel far questo il legislatore ha preferito ricondurre i nuovi reati alle figure già esistenti invece che prevedere un apposito titolo ad hoc.
Non sono poi state previste contravvenzioni, in quanto si è ritenuto che tra le figure inserite non vi siano ipotesi alle quali destinare norme di carattere preventivo, né fattispecie concernenti la disciplina di attività soggette ad un potere amministrativo[11].
L'unico aspetto lasciato scoperto dalla normativa in esame è quello relativo alla tutela delle persone rispetto al trattamento dei dati personali. Tale lacuna è stata colmata in un primo

---

8 Relazione Introduttiva al Disegno di Legge n.2773. Per cogliere l'intenzione del legislatore, si fa riferimento alla relazione introduttiva del disegno di legge in quanto l'articolato su cui si discute riprende interamente lo stesso, assorbendo, nei limiti in cui con questo non contrastava, la proposta di legge Cicciomessere ed altri: *Introduzione degli articoli 623-ter, 623-quater, 623-quinquies, 623-sexies e 623-septies del codice penale per la repressione dei reati informatici e telematici* (n.1174). Sul furto dei dati cfr. E.Giannantonio, *Manuale di Diritto dell'Informatica*, op.cit, p.419 ss..

9 Relazione Introduttiva al Disegno di Legge n. 2773.

10 Fondamentale in materia è l'elencazione dei reati informatici proposta dal Comitato ristretto degli esperti sulla criminalità informatica del Consiglio d'Europa.

11 Il legislatore ha ritenuto così di rispettare i criteri orientativi dettati dalla circolare della Presidenza del Consiglio, 5 febbraio 1986.

momento attraverso la l. 31 dicembre 1996 n. 675 e successivamente mediante il Codice in materia di protezione dei dati personali.
Accanto alla legge 547/93 si individuano, inoltre, altre norme riferite a reati commessi attraverso le tecnologie dell'informazione.
La divulgazione e cessione telematica di materiale pedopornografico e la sua detenzione nel sistema informatico sono punite rispettivamente dagli art. 600 ter e 600 quater c.p. (disposizioni introdotte nel codice penale dalla legge 3 agosto 1998, n.269 "Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di riduzione in schiavitù", successivamente modificata dalla l. 38/2006 contenente disposizioni in tema di lotta contro lo sfruttamento sessuale dei bambini e pedopornografia).
L'assistenza a gruppi terroristici apprestata fornendo strumenti di comunicazione e, quindi, anche telematici, assume rilevanza penale in virtù di quanto disposto dall'art. 270 ter c.p. (inserito nel codice penale dalla legge 15 dicembre 2001, n.438, che ha convertito in legge, con modificazioni, il decreto-legge 18 ottobre 2001, n.374, recante disposizioni urgenti per contrastare il terrorismo internazionale).

7. La legge 23 dicembre 1993 n. 547

La legge 547 del 1993 ha il merito di aggiornare il codice penale ampliando la portata delle norme preesistenti ed aggiungendone di nuove.[12]
L'art.1 integra l'art. 392 cod. pen., prevedendo che il reato di esercizio arbitrario delle proprie ragioni con violenza sulle cose comprenda anche una fattispecie di violenza sulle cose realizzata attraverso il danneggiamento di software o l'impedimento del funzionamento di un sistema informatico;
L'art. 2 interviene in tema di delitti contro l'ordine pubblico, prevedendo che il delitto di attentato ad impianti di pubblica utilità (art. 420 cod. pen.) riguardi anche l'ipotesi di danneggiamento o distruzione di sistemi informatici o telematici di pubblica utilità oppure di dati e del software in essi contenuti.
L'art. 3, che aggiunge al codice penale l'art. 491-bis, consente la tutela penale del documento informatico.
L'art. 4, che introduce all'interno del cod. pen. gli artt.615-ter, quater e quinquies, permette di punire ipotesi totalmente nuove quali l'accesso abusivo ad un sistema informatico o telematico, la detenzione e diffusione abusiva di codici di accesso e la diffusione di programmi diretti a danneggiare o interrompere un sistema informatico.
Gli artt. 5, 6, 7 e 8 tutelano l'inviolabilità dei segreti: il primo integra l'art.616 cod. pen. riferendolo anche alla violazione, sottrazione e soppressione della corrispondenza informatica. Il secondo aggiunge tre nuove fattispecie di reato: l'intercettazione, l'impedimento e l'interruzione illecita di comunicazioni informatiche e telematiche (art. 617-quater); l'installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche (art.

12 Per un approfondimento sulle novità apportate dalla legge n.547 cfr C.Pecorella, Il diritto penale dell'informatica, Cedam, Padova, 2000.

617-quinquies); la falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche e telematiche (art. 617-sexies).
L'art.7 modifica l'art. 621 cod. pen., relativo alla rivelazione del contenuto di documenti segreti, includendo tra i documenti segreti anche i supporti informatici contenenti dei dati.
Attraverso l'art 8, infine, si introduce con l'art.623-ter cod. pen., una norma di chiusura statuente che le norme penali della sezione V del codice penale, relative ai delitti contro l'inviolabilità dei segreti, si applichino anche ad ogni altra trasmissione a distanza di suoni, immagini o altri dati.
Gli articoli 9 e 10 riguardano i delitti contro il patrimonio. Il primo introduce una fattispecie speciale di danneggiamento, riferito al danneggiamento di sistemi informatici e telematici (art. 635-bis); il secondo introduce la nuova fattispecie di frode informatica (art. 640-ter), nella quale il sistema informatico non è solo l'oggetto del reato, ma anche lo strumento con il quale viene leso il patrimonio della vittima della frode. Gli articoli 11,12 e 13 recano, infine, modifiche al codice di procedura penale.
Dalla lettura della legge risulta evidente come il legislatore italiano abbia optato per il metodo evolutivo ritenendo, a ragione, che le tecnologie incidano sulle modalità di aggressione a beni giuridici o interessi che rimangono comunque invariati.
Ne consegue che a differenza di altri Paesi, es. gli Stati Uniti o la Francia, che hanno rispettivamente dedicato ai delitti informatici leggi *ad hoc* e titolo apposito all'interno del codice penale, in Italia le nuove norme sono state inserite in diversi parti del codice penale, ciascuna vicino alla norma previgente ritenuta simile.

8. La legge 18 marzo 2008, n. 48

Le modifiche apportate al codice penale attraverso la legge 547 si sono arricchite di recente di contenuti nuovi grazie alla legge 18 marzo 2008, n.48 "Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento interno".[13]
Con la Convenzione per la lotta contro la criminalità informatica si era stilato un documento ispirato dalla convinzione che i nuovi fenomeni potevano essere ben contrastati solo attraverso una armonizzazione delle legislazioni, che tenesse conto della dimensione transnazionale dei crimini informatici.
In questa prospettiva si era ribadita l'esigenza di prevedere nelle legislazioni interne norme penali idonee a sanzionare determinate condotte, disposizioni processuali capaci di rendere effettivamente punibili i reati previsti, previsioni normative che contemplassero finalmente una responsabilità delle aziende per reati informatici commessi al loro interno.
Nel recepire tali indicazioni la legge n.48 opera sostanzialmente su tre piani: quello del diritto sostanziale, processuale e della rilevanza penale di alcune condotte in ambito aziendale. Quanto

[13] Sul contenuto della Convenzione cfr C.Sarazana, *Informatica, internet e diritto penale*, Giuffrè, Milano, 2010, p.587 ss.

a tale ultimo profilo si estende alle aziende la responsabilità amministrativa già prevista per numerosi reati dal Decreto legislativo 231 a praticamente tutti i delitti informatici commessi dai vertici o dai dipendenti, sempre che siano realizzati nell'interesse dell'ente o per l'ipotesi che lo stesso ne abbia tratto un vantaggio.

Importanti novità si registrano anche nell'ambito del diritto sostanziale. [14]

L'art. 615 quinquies, originariamente volto a sanzionare *la diffusione di programmi diretti a danneggiare o interrompere un sistema informatico*, reprime oggi *la diffusione di apparecchiature, dispositivi o programmi informatici diretti danneggiare o interrompere un sistema informatico*. La norma, così come novellata, punisce, quindi, *chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, si procura, riproduce, importa, diffonde, comunica consegna o, comunque mette a disposizione di altri apparecchiature, dispositivi o programmi informatici aventi per scopo o per effetto il danneggiamento di un sistema informatico o telematico, delle informazioni, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento.*

Si prevedono poi più ipotesi di danneggiamento informatico e segnatamente:

il danneggiamento di informazioni, dati e programmi informatici (art.635 bis); il danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635 ter); il danneggiamento di sistemi informatici e telematici (art. 635 quater); il danneggiamento di sistemi informatici e telematici di pubblica utilità (art. 635 quinquies).

Le maggiori novità attengono, tuttavia, alla disciplina penale del documento informatico e della firma digitale. In tale direzione si registra l'eliminazione della definizione di documento informatico introdotta dalla legge 547 del 93, per dar spazio a quella più corretta già contenuta nel regolamento di cui al Decreto del Presidente del Repubblica 10 novembre 1997, n.513 e ripresa dal Codice dell'amministrazione digitale. Anche ai fini penalistici, quindi, per documento informatico non si intenderà più "il supporto informatico contenente dati o informazioni aventi efficacia probatoria", bensì "la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti". Opportuna risulta poi l'introduzione dei reati di falsa dichiarazione o attestazione al certificatore sull'identità o su qualità personali proprie o di altri (art.495 bis) e di truffa del certificatore di firma elettronica (art.640 quinquies).

Interessanti novità si registrano, infine, in ambito processuale, atteso che sino ad oggi i maggiori problemi applicativi delle norme sulla criminalità informatica dipendevano proprio dalla poca chiarezza in ordine a ciò che gli organi inquirenti potevano fare nella delicata fase dell'accertamento del reato.[15] Si prevede oggi espressamente la possibilità per l'autorità giudiziaria di disporre, in sede di ispezione, rilievi e altre operazioni tecniche sui sistemi, di perquisire gli stessi anche se protetti da misure di sicurezza, di esaminare presso le banche anche i dati, le informazioni ed i programmi informatici. E' contemplata altresì una disciplina sulle modalità di acquisizione dei dati oggetto di sequestro presso i fornitori di servizi informatici e telematici o di telecomunicazioni, nonché un provvedimento che permetta il congelamento temporaneo ed urgente dei dati personali. Viene prevista, infine, la concentrazione della

---

[14] Sull'argomento cfr P.G. Demarchi, (a cura di), *I nuovi reati informatici,* G. Giappichelli, Torino, 2009, p.7 ss.

[15] Sull'argomento cfr P.G. Demarchi, (a cura di), *I nuovi reati informatici,* G. Giappichelli, Torino, 2009, p.47 ss.

competenza per i reati informatici presso gli uffici di procura distrettuali al fine di facilitare il coordinamento delle indagini e la formazione di gruppi di lavoro specializzati in materia.

9. Il reato informatico in azienda alla luce delle modifiche apportate dalla legge 18 marzo 2008, n.48

Inizialmente le aziende non erano particolarmente interessate alla legislazione penale dell'informatica "forti" del fatto che, essendo la responsabilità penale personale, in caso di reato avrebbe risposto il suo autore. La situazione è radicalmente mutata ultimamente in quanto a seguito delle modifiche apportate al Decreto legislativo 231 dalla l. n. 48 del 2008 l'azienda può essere chiamata a rispondere per la maggior parte dei reati informatici commessi dai suoi vertici e dipendenti.[16]
La legge n.48, infatti, estende (art7) la responsabilità amministrativa degli enti ai seguenti reati informatici:

- falsità in un documento informatico (art. 491-bis c.p.);
- accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.);
- detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater c.p.);
- diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.);
- intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.);
- installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 615-quinquies c.p.);
- danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.);
- danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-ter c.p.);
- danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.);
- danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p.);
- frode informatica del certificatore di firma elettronica (art. 640-quinquies c.p.).

Si tratta di una grande novità atteso che fino ad oggi sulla base del Decreto Legislativo 231/01 tale responsabilità era prevista solo per residuali ipotesi di reato informatico, quali quelli di

[16] Sulle problematiche poste dai reati informatici commessi in azienda cfr: P.Galdieri, C.Giustozzi, M.Strano, *Sicurezza e privacy in azienda*, Apogeo, Milano, 2001; I.Corradini, *Il crimine informatico in azienda*, in *Tecnologie dell'informazione e comportamenti devianti*, Gemma Marotta (a cura di), LED, Milano, 2004 p.75 e ss.

frode informatica commessa a danno dello Stato o di altro Ente pubblico, di assistenza a gruppi terroristici apprestata fornendo strumenti di comunicazione, di distribuzione, cessione e detenzione di materiale pedopornografico.
Ciò che può preoccupare le aziende poi non è solo l'estensione di tale responsabilità a tutti i delitti informatici, ma la circostanza che la stessa possa essere imputata anche nelle ipotesi in cui non venga rintracciato l'autore materiale del reato. Ne consegue che la mancata individuazione del soggetto attivo del reato, non infrequente in materia di criminalità informatica, possa non far comprendere esattamente all'organo giudicante le motivazioni dello stesso e quindi determinare un'attribuzione di responsabilità anche quando l'autore del reato abbia agito per fini esclusivamente personali e non nell'interesse del suo datore di lavoro.
La preoccupazione non può poi che aumentare quando si consideri che l'azienda ritenuta responsabile è soggetta oltre che all'esborso di ingenti somme di danaro a sanzioni interdittive quali: a) l'interdizione dall'esercizio dell'attività; b) la sospensione o la revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; c) il divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio; d) l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; e) il divieto di pubblicizzare beni o servizi.
Di fronte a tale nuovo scenario l'azienda è inevitabilmente costretta a studiare delle strategie preventive idonee, da un lato, ad impedire la commissione di reati informatici al suo interno e dall'altro, capaci di escluderne una sua responsabilità nelle ipotesi in cui le misure adottate non siano state in grado di evitare la commissione del reato.
Per limitare al massimo la commissione di reati nel contesto aziendale occorre sicuramente partire da una responsabilizzazione di tutti i soggetti che ivi lavorano, cosa che si può ottenere attraverso strumenti diversi.
Assai utile può rivelarsi la predisposizione di corsi di formazione interna in grado di spiegare ai vertici ed ai dipendenti dell'azienda ciò che si può e ciò che non si deve fare con gli strumenti informatici. Corsi di formazione la cui efficacia dipenderà molto dalla conoscenza preventiva del modo di lavorare e di pensare di ciascuno, conoscenza questa acquisibile attraverso la compilazione di questionari anonimi in grado "di far sentire il polso dell'azienda" a colui che è chiamato a formare.
Altrettanto efficace potrebbe poi rivelarsi la redazione di un vero e proprio codice di comportamento informatico, i cui principi fondamentali potrebbero essere addirittura inseriti all'interno del contratto di lavoro.
L'adozione di tali soluzioni potrebbero quindi servire per dimostrare "in prima battuta" che si è fatto tutto ciò che era possibile per impedire che propri dipendenti commettessero un reato informatico e quindi evitare una sorta di responsabilità per *culpa in vigilando*.
Parimenti, per respingere rimproveri per una forma di *culpa in eligendo* sarà indispensabile affidare incarichi "delicati" connessi all'uso dei sistemi informatici a soggetti dotati di specifiche competenze.
D'altra parte tali accorgimenti vanno proprio nella direzione del Decreto Legislativo 231 del 2001, che prevede l'esonero di una responsabilità dell'ente allorquando lo stesso dimostri di aver predisposto modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi.

A tal proposito si distingue a seconda che il reato venga commesso da un vertice o da un dipendente.
Nella prima ipotesi l'ente non risponde del reato commesso quando sia in grado di dimostrare che:

- l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi;
- il compito di vigilare sul funzionamento e l'osservanza dei modelli di curare il loro aggiornamento è stato affidato ad un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo;
- le persone hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione e di gestione;
- non vi è stata omessa o insufficiente vigilanza da parte dell'organismo di controllo.

Ovviamente non basta redigere il predetto modello organizzativo essendo necessario che lo stesso risponda alle seguenti esigenze:

- individuare le attività nel cui ambito possono essere commessi reati;
- prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire;
- individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati;
- prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli;
- introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

Per agevolare il compito delle aziende si prevede che i modelli possano essere adottati sulla base di codici di comportamento redatti dalle associazioni rappresentative degli enti, comunicati al Ministero della giustizia che, di concerto con i Ministeri competenti, può formulare, entro trenta giorni, osservazioni sulla idoneità dei modelli a prevenire i reati.
Negli enti di piccole dimensioni il compito di vigilare sul funzionamento e l'osservanza dei modelli, nonché di curarne il loro aggiornamento, può essere svolto direttamente dall'organo dirigente.
Riguardo ai soggetti sottoposti all'altrui direzione, sempre secondo il Decreto legislativo 231, l'ente è responsabile se la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione o vigilanza.
In ogni caso, è esclusa l'inosservanza di tali obblighi se l'ente, prima della commissione del reato, ha adottato ed efficacemente attuato un modello di organizzazione, gestione e controllo idoneo a prevenire reati della specie di quello verificatosi.
Il modello, in questo caso, prevede, in relazione alla natura e alla dimensione dell'organizzazione nonché al tipo di attività svolta, misure idonee a garantire lo svolgimento dell'attività nel rispetto della legge e a scoprire ed eliminare tempestivamente situazioni di rischio.
Ne consegue che l'efficace attuazione del modello richiede:

- una verifica periodica e l'eventuale modifica dello stesso quando sono scoperte significative violazioni delle prescrizioni ovvero quando intervengano mutamenti nell'organizzazione

o nell'attività;
- un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

Se la novità introdotta dalla legge in commento finisce con il gravare ancora di più di oneri e responsabilità il comparto aziendale, è pur vero che tale scelta era in qualche modo obbligata considerando che tale tipo di responsabilità era già stata prevista per molti delitti non informatici e visto che rispetto a quelli informatici queste erano da tempo le indicazioni comunitarie.

10. La strategia comunitaria per contrastare la criminalità informatica

La criminalità informatica, ha oramai natura transnazionale, nel senso che gravita in una dimensione virtuale, pensiamo alla rete Internet, senza vincoli temporali e soprattutto di spazio.

Ne deriva dal punto di vista giuridico l'esigenza di un coordinamento delle legislazioni interne da realizzarsi attraverso gli organismi sovranazionali.

Volendo concentrare l'attenzione sugli orientamenti dell'Unione Europea, e tralasciando, quindi, quelli di altri organismi parimenti importanti, è possibile individuare due tipi di intervento.

Il primo ha come scopo precipuo quello della sicurezza della rete, anche al fine di favorire la circolazione dei beni e servizi all'interno di Internet. Primo passo fondamentale per realizzare questo disegno si registra il 24 aprile 1996, quando il Consiglio chiede alla Commissione di redigere un compendio dei problemi posti dal rapido sviluppo di Internet e di valutare, in particolare, l'opportunità di una disciplina comunitaria o internazionale. Successivamente, il 24 ottobre 1996, la Commissione trasmette al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale e al Comitato delle Regioni una Comunicazione relativa alle informazioni di contenuto illegale e nocivo su Internet e un Libro Verde sulla tutela dei minori e della dignità umana nei servizi audiovisivi e dell'informazione. Recepita la Comunicazione, con la Risoluzione del 17 febbraio 1997 il Consiglio e i rappresentanti dei governi degli Stati membri, riuniti in sede di Consiglio, hanno chiesto agli Stati membri e alla Commissione di intraprendere una serie di azioni per difendere Internet dai contenuti illegali e nocivi. Nell'ambito di questa strategia si inserisce la Dichiarazione Ministeriale, adottata alla Conferenza ministeriale internazionale sulle "Reti globali di informazione: realizzare il potenziale", tenutasi a Bonn il 6-8 luglio 1997 su iniziativa del governo tedesco, che sottolinea il ruolo che il settore privato può assumere nella tutela degli interessi dei consumatori e nella promozione e nel rispetto degli standards etici, grazie ad efficaci sistemi di autoregolamentazione conformi al sistema giuridico e da esso sostenuti. La stessa Dichiarazione Ministeriale incoraggia gli operatori ad adottare sistemi di classificazione del contenuto, aperti ed indipendenti dalle piattaforme, ed a proporre servizi di classificazione adeguati alle esigenze dei vari utenti e al pluralismo culturale e linguistico europeo; riconosce, inoltre, l'importanza di diffondere sicurezza e fiducia nelle

reti globali di informazione mediante il rispetto dei diritti fondamentali dell'uomo e attraverso la salvaguardia degli interessi delle società in generale, compresi quelli dei produttori e dei consumatori.
Altro atto della strategia adottata in ambito europeo è costituito dalla Decisione 276/1999 CE del Parlamento Europeo e del Consiglio del 25 gennaio 1999, con la quale viene adottato il piano pluriennale d'azione comunitario per promuovere l'uso sicuro di Internet attraverso la lotta alle informazioni di contenuto illegale e nocivo diffuse per mezzo delle reti globali.
Si tratta di un piano particolarmente ambizioso con una durata di quattro anni, dal 1 gennaio 1999 al 31 dicembre 2002, finalizzato a promuovere l'uso sicuro di Internet e ad incoraggiare a livello europeo un ambiente favorevole allo sviluppo del settore relativo.
Le linee di azione hanno i seguenti obiettivi: 1) invitare i soggetti interessati (operatori, utenti) a sviluppare ed applicare adeguati sistemi di autoregolamentazione; 2) incentivare gli sviluppi, sostenendo le dimostrazioni e stimolando l'applicazione di soluzioni tecniche; 3) avvisare ed informare genitori ed insegnanti, soprattutto attraverso le loro rispettive associazioni; 4) stimolare la cooperazione e lo scambio di esperienze e delle migliori pratiche a livello europeo ed internazionale; 5) promuovere il coordinamento a livello europeo e tra i soggetti interessati; 6) garantire la compatibilità tra l'approccio seguito in Europa e quello seguito altrove.
Rientrano in questa strategia: l'istituzione di una rete europea di hot lines; la sollecitazione all'autoregolamentazione ed all'uso di codici di condotta; lo sviluppo di sistemi di filtraggio e di classificazione.
Sempre in quest'ambito si collocano la Decisione 854/2005/CE del Parlamento europeo e del Consiglio dell'11 maggio 2005, che istituisce un programma comunitario pluriennale inteso a promuovere un uso più sicuro di Internet e delle nuove tecnologie *online* e la Decisione n.1351/2008/CE del Parlamento europeo e del Consiglio, del 16 dicembre 2008, relativa a un programma comunitario pluriennale per la protezione dei bambini che usano internet e le altre tecnologie di comunicazione.
Altro tipo di intervento è quello finalizzato a limitare al massimo la diffusione della criminalità informatica.
In tale direzione si muovono i seguenti documenti: la Raccomandazione del Consiglio d'Europa R (89) 9, attraverso la quale si invitano i Paesi membri a prevedere nuove ipotesi di reato aventi ad oggetto l'informatica[17], al fine di consentire un'effettiva cooperazione internazionale; la Raccomandazione R (95)13, che sollecita l'adeguamento dei codici di procedura penale ai recenti sviluppi delle tecnologie dell'informazione, in modo che i nuovi reati previsti dai singoli Stati membri possano realmente essere perseguiti; il Parere del Comitato consultivo "*razzismo e xenofobia del 26 gennaio 1996 "sulla diffusione dell'odio razziale mediante mezzi informatici o telematici*"; la Risoluzione del 9 maggio 1996 sulla proposta di decisione del Consiglio, che proclama il 1997 "anno europeo contro il razzismo", nonché l'azione comune del 15 luglio 1996 adottata dal Consiglio; il Libro Verde della Commissione sulla protezione dei minorenni e della dignità umana nei servizi audiovisivi e d'informazione del 29 novembre 1996.
Di estremo interesse è, anche la Comunicazione della Commissione europea "*Creare una società*

[17] V. Frosini, *Contributi ad un diritto dell'informazione*, op.cit, p. 165 ss.

dell'informazione sicura, migliorando la sicurezza delle infrastrutture dell'informazione e mediante la lotta alla criminalità informatica" (COM-2000-890.) [18] in cui si individuano le questioni più delicate poste dalla cybercriminalità, avanzando proposte legislative ed extragiuridiche.
L'esigenza di contrastare la criminalità informatica traspare anche da altri documenti come quello, pubblicato nella Gazzetta Ufficiale dell'Unione Europea, intitolato "Prevenzione e controllo della criminalità organizzata" (2000/C124/01), che, nel fare il punto sulle strategie dell'Unione Europea per l'inizio del terzo millennio, dichiara esplicitamente la necessità di avvicinare ed armonizzare le legislazioni nazionali dei Paesi membri su alcuni reati, tra cui quelli legati alla diffusione delle nuove tecnologie.
Tale necessità si riflette in modo ancora più evidente nella Convenzione del Consiglio d'Europa sulla Cybercriminalità (Budapest, 23 novembre 2001) i cui scopi sono: armonizzare le legislazioni; fornire al diritto processuale nazionale i poteri necessari al perseguimento di questa tipologia di reati; mettere in piedi un regime di efficace cooperazione internazionale.

11. L'interpretazione del delitto informatico

Le norme penali che contemplano reati informatici, pur diverse tra loro, presentano alcune caratteristiche comuni.
In primo luogo esse si differenziano nel contenuto da quelle previgenti, in quanto utilizzano termini tecnici sino ad oggi non presenti nelle disposizioni di legge. Si pensi a tal proposito a continui richiami a termini quali "sistema informatico e telematico", "programma informatico", " dato e informazione", "misure di sicurezza".
In secondo luogo si riferiscono a condotte nuove, non immaginabili sino a pochi anni fa. Pensiamo all'accesso abusivo all'interno di un sistema informatico o alla diffusione di *virus* informatici, che si realizzano e pongono problemi sensibilmente diversi da quelli posti sino ad oggi dalle attività delittuose già note.
In terzo luogo trovano applicazione in contesti anch'essi modificati. Un reato commesso in un'azienda non automatizzata pone, infatti, problemi differenti da quelli che determina all'interno di un'impresa la cui attività è totalmente gestita dagli elaboratori.
Infine si riferiscono, talvolta, a comportamenti che non sono soltanto diversi sotto il profilo oggettivo, ma anche sotto il profilo soggettivo. E'indubbio, infatti, che determinate azioni sono realizzate perché le tecnologie offrono nuove opportunità, per es. quella di mantenere l'anonimato, così come alcune condotte trovano ispirazione proprio da quel confronto-scontro con le tecnologie: è il caso di alcuni *hackers* che entrano nei sistemi altrui con il fine esclusivo di contrastare, a loro dire, una nuova forma di potere definita appunto "potere informatico".
Caratteristiche analoghe a quelle sinora descritte si rinvengono nelle norme "tradizionali" allorquando le stesse sono applicate a condotte informatiche. Pensiamo al delitto di diffamazione commesso attraverso Internet. La norma che trova applicazione è l'art. 595 c.p.,

[18] Il testo integrale è consultabile in: www.privacy.it/com2000-890.

che non si riferisce espressamente al mezzo telematico, ciononostante, allorquando essa va applicata ad ipotesi dove è coinvolta la rete, si ripropongono problemi derivanti direttamente dal mezzo impiegato per commettere il reato, ad es. quello dell'individuazione del luogo del commesso reato.
Caratteristiche comuni, e quindi problemi particolari, pongono anche quelle norme del codice di procedura penale che consentono agli organi inquirenti di contrastare i reati commessi attraverso le tecnologie dell'informazione (es. norme che si riferiscono alle intercettazioni informatiche e telematiche o al sequestro probatorio dei *computers*).
Dall'interpretazione delle norme, delle condotte cui le stesse si riferiscono, del contesto in cui le disposizioni di legge vanno applicate, dipende l'esito stesso del procedimento penale instaurato.
Volendo indagare sui problemi interpretativi posti da ciascuno degli elementi indicati pare opportuno affrontarli seguendo l'iter di un procedimento penale che, come noto, si compone di due fasi fondamentali ovvero quella delle indagini preliminari e quella dell'eventuale conseguente giudizio, intendendo con quest'ultimo riferirci anche all'eventuale giudizio di appello e di Cassazione.
Nella prima fase gli organi inquirenti e quindi il P.M., coadiuvato dalle forze di polizia, si muovono alla ricerca di quegli elementi che possono risultare utili per sostenere l'accusa all'interno del processo. Nella seconda fase, quella del giudizio, ruolo centrale viene ricoperto dall'organo giudicante (Tribunale, Corte d'Appello, Cassazione), il quale dovrà confrontarsi con le norme, anche alla luce delle tesi prospettate dall'accusa e dalla difesa.
Nel corso delle indagini preliminari i problemi posti dai reati informatici da analizzare sono principalmente quelli delle modalità di acquisizione delle prove, sul piano fattuale e giuridico; nella fase del giudizio le questioni poste dai delitti informatici sono riconducibili al contenuto delle norme, delle condotte e dei contesti, ovvero a tutti quegli elementi dei quali il giudice dovrà tener conto ai fini del decidere.

12. Il delitto informatico nelle indagini preliminari

In tema di indagini preliminari aventi ad oggetto i reati informatici è possibile svolgere alcune considerazioni di carattere generale.[19]
La prima è che nel volgere di alcuni anni si è giunti ad una adeguata preparazione, anche sotto il profilo tecnico, da parte degli organi inquirenti e delle forze dell'ordine.
Nelle prime esperienze investigative si è pagato lo "scotto" di un'insufficiente esperienza delle forze dell'ordine e di una normativa in tema di indagini informatiche non ancora ben collaudata.
E' questo il periodo in cui si registrano sequestri immotivati di oggetti per nulla attinenti al

[19] Sull'argomento cfr: R.Di Pietro, G. Me, *Le investigazioni informatiche nel processo penale,* in *Tecnologie dell'informazione e comportamenti devianti*, Gemma Marotta (a cura di), LED, Milano, 2004 p.239 ss.; L.Luparia, G. Ziccardi, *Investigazione penale e tecnologia informatica,* Giuffrè, Milano, 2007, p.31 ss.; L. Luparia (a cura di), *Sistema penale e criminalità informatica,* Giuffrè, Milano, 2009, p.113 ss.

thema probandum ad es. di tappetini e mouse: si è arrivati ad apporre i sigilli nella camera da letto dove si trovava un computer, non sapendo cosa fare in assenza di specifiche disposizioni da parte del Pubblico Ministero!
Attualmente all'interno delle forze dell'ordine sono state create sezioni altamente specializzate, ciascuna con specifiche competenze tecniche.
Nella Polizia di Stato opera la Polizia Postale che comprende al suo interno una particolare sezione deputata ad indagare sui crimini informatici.
Nell'ambito del Raggruppamento Carabinieri Investigazioni Scientifiche (Ra.C.I.S.) vi è la sezione telematica incaricata di svolgere indagini relative ai reati commessi attraverso le tecnologie. Indagini altamente qualificate in materia vengono svolte anche dal Nucleo Speciale Anticrimine Tecnologico della Guardia di Finanza.
La seconda considerazione è che i diversi problemi che si incontrano nelle indagini aventi ad oggetto crimini informatici, traggono tutti origine dalla natura stessa dei delitti oggetto di investigazione, che pone questioni peculiari in ordine al suo concreto accertamento, all'individuazione del suo autore, nonché al modo stesso in cui vanno acquisiti gli elementi probatori.
La terza considerazione è che la natura stessa della rete, idonea a mettere in contatto soggetti che neanche si conoscono tra loro, favorisce la nascita di procedimenti a carico di numerosi coindagati: basti pensare alle continue "maxi retate" in tema di pedofilia telematica.
A prescindere da valutazioni di merito, che presupporrebbero la conoscenza degli atti del singolo procedimento, rileva come in linea generale un procedimento con tanti indagati per delitti che si prescrivono al massimo in sette anni e mezzo è destinato "a morire" ancor prima di emettere "il primo vagito". Rispetto ai reati per i quali è più diffusa la pratica di maxi operazioni, ovvero quelli di divulgazione di materiale pedopornografico, si registra l'ulteriore rischio di tralasciare aspetti che destano un maggiore allarme sociale, ad esempio gli abusi sessuali, per dedicarsi al contrasto di fenomeni che, seppure deprecabili, manifestano un minore disvalore sociale.[20]
Quarta considerazione è che in tema di indagini informatiche sovente si registra un affievolimento delle garanzie dell'indagato.
Benchè, come detto, sia nettamente migliorata la competenza tecnica da parte delle forze dell'ordine, ancora troppo spesso si assiste a perquisizioni e sequestri privi di adeguata motivazione.
Prassi sicuramente censurabile, poi, è quella di restituire il materiale ritenuto superfluo ai fini delle indagini con grande ritardo e sovente con ingiustificato danno per l'indagato.
Tuttavia, la maggiore compressione delle garanzie dell'indagato non è dovuta tanto alle indagini in sé, ma alla pubblicizzazione che delle stesse viene fatta dagli organi d'informazione. Si pensi, a titolo di esempio, alle continue notizie fornite dai media su indagini in corso in materia di pedofilia telematica, la cui risonanza ha spinto, purtroppo, in alcuni casi l'indagato addirittura a togliersi la vita.

---

[20] Sull'argomento cfr G.S.Manzi, *Brevi cenni sui metodi di investigazione nella pornografia minorile,* in *Tecnologie dell'informazione e comportamenti devianti*, Gemma Marotta (a cura di), LED, Milano, 2004 p.221 ss.

Posto che qualunque fatto di cronaca trovi legittimo accesso nei canali della informazione, perché grave sarebbe il contrario, è altresì necessario apprestare adeguata cautela allorquando si forniscono informazioni su procedimenti dall'esito ancora incerto.
Il problema di carattere generale, perché riferibile a qualsiasi tipo di indagine, assume connotati peculiari in tema di criminalità informatica.
È agevole a tal riguardo constatare come i reati commessi attraverso le tecnologie suscitino interesse nell'opinione pubblica, e talvolta addirittura simpatia, così da divenire argomento ben gradito dai fruitori delle informazioni e, quindi, da coloro che dalla diffusione delle informazioni traggono utili economici.

13. I mezzi di ricerca della prova

Momento centrale della fase delle indagini è sicuramente quello della ricerca della prova necessaria a sostenere un eventuale accusa all'interno del processo.
I mezzi di ricerca della prova sono disciplinati dal titolo III, libro terzo del codice di procedura penale, che considera tali le ispezioni (artt. 244-246), le perquisizioni (artt. 247-252), i sequestri (artt. 253-265), le intercettazioni (artt. 266-271).
Di queste norme espressamente riferita alla realtà informatica è l'art. 266 bis " Intercettazioni di comunicazioni informatiche e telematiche", introdotta dall'art. 11 della l.23 dicembre 1993 n.547, che consente l'intercettazione del flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi, oltre che rispetto ai delitti per i quali è consentita l'intercettazione telefonica, anche per i reati commessi mediante le tecnologie informatiche o telematiche.
Tali intercettazioni, sulla base di quanto disposto dal comma 3 bis dell'art. 268 c.p.p.- a differenza di quanto avviene per quelle telefoniche dove l'operazione deve essere di regola compiuta mediante impianti installati nella procura della Repubblica, salvo che tali impianti risultino insufficienti o inidonei ed esistano ragioni di urgenza, nel qual caso il p.m. può disporre con provvedimento motivato il compimento delle operazioni mediante impianti di pubblico servizio o in dotazione alla polizia giudiziaria-, possono essere compiute anche mediante impianti appartenenti a privati su disposizione del Pubblico Ministero.
Norme fondamentali ai fini dell'indagine e segnatamente riferite alla realtà informatica sono poi l'art. 14 della legge 269/98, in materia di delitti legati all'abuso e sfruttamento sessuale dei minori e l'art. 4 della legge 15 dicembre 2001 n. 438 (che ha convertito con modificazioni, in legge il Decreto-legge 18 ottobre 2001, n.374 "Disposizioni urgenti per contrastare il terrorismo internazionale) in tema di contrasto al terrorismo.
Tralasciando di esaminare la portata di tali norme, preme evidenziare come le maggiori questioni attinenti i mezzi di ricerca della prova riguardavano sino ad oggi le modalità attraverso le quali si perveniva al sequestro dei *computer*s.
Il problema nasceva poiché non esisteva nel nostro ordinamento una norma espressamente riferita al sequestro dei *computers* e quindi occorreva di volta in volta verificare le conseguenze di una disciplina pensata per beni che hanno caratteristiche sensibilmente diverse da quelle proprie dei sistemi informatici.

Tale problema potrebbe oggi attenuarsi grazie alle novità introdotte dalla l. n 48 del 2008, che prevede espressamente la possibilità per l'Autorità giudiziaria di disporre, in sede di ispezione, rilievi e altre operazioni tecniche sui sistemi, di perquisire gli stessi anche se protetti da misure di sicurezza, di esaminare presso le banche anche i dati, le informazioni ed i programmi informatici. E' contemplata altresì una disciplina sulle modalità di acquisizione dei dati oggetto di sequestro presso i fornitori di servizi informatici e telematici o di telecomunicazioni, nonché un provvedimento che permetta il congelamento temporaneo ed urgente dei dati personali. Viene prevista, infine, la concentrazione della competenza per i reati informatici presso gli uffici di procura distrettuali al fine di facilitare il coordinamento delle indagini e la formazione di gruppi di lavoro specializzati in materia.

14. L'interpretazione del reato informatico da parte degli organi giudicanti

Il rapporto che intercorre tra diritto penale e tecnologie dell'informazione si arricchisce di contenuti allorquando lo si valuta sul piano concreto ovvero facendo riferimento all'interpretazione svolta sulle singole norme dal giudice.
Da questo punto di vista un primo dato che emerge è che la normativa penale riferibile alle tecnologie va a disciplinare un contesto nato e sviluppatosi in assenza di regolamentazione, favorendo così il convincimento che determinate condotte siano pienamente legittima. Conseguenza è che molti dei divieti posti nel volgere di pochi anni possano non essere compresi e, talvolta, considerati addirittura ingiusti. In tale ottica si pongono le azioni dimostrative di alcuni *hackers* che agiscono al sol fine, almeno a loro dire, di contrastare un sistema volto a favorire e preservare regimi di monopolio ed oligopolio in materia di produzione delle tecnologie e controllo dell'informazione.
Altro dato è che la norma pare sovente rivolta alla tutela di interessi economici, che potrebbero trovare più adeguata protezione attraverso norme di natura civilistica. Tale obiezione viene mossa ad alcune delle disposizioni penali introdotte all'interno della legge sul diritto d'autore per contrastare condotte illecite aventi ad oggetto il programma informatico e realizzabili anche attraverso la rete. Per l'ambito di nostro interesse rileva come la previsione della sanzione penale per la duplicazione abusiva "per fine di profitto", che consente di punire anche chi duplica per fini personali, pare sproporzionata tanto rispetto alla tipologia di danno arrecato che rispetto al reale disvalore sociale della condotta. Discutibile è la previsione di sconti di pena per colui che prima che la violazione gli sia specificatamente contestata in un atto dell'autorità giudiziaria, la denuncia spontaneamente o, fornendo tutte le informazioni in suo possesso, consente l'individuazione del promotore o organizzatore dell'attività illecita, di altro duplicatore o distributore, ovvero il sequestro di notevoli quantità di supporti, strumenti o materiali serviti o destinati alla commissione dei reati. E' agevole in tal caso evidenziare la sproporzione nell'utilizzo di uno strumento, "il pentitismo", sicuramente più adatto e ragionevole per contrastare fenomeni ben più pericolosi quali mafia, traffico di sostanze stupefacenti e terrorismo.

Lo spostamento di interesse dalle libertà fondamentali agli interessi economici è testimoniato da altre disposizioni di legge. Sintomatico di tale impostazione è il fatto che il Codice in materia di protezione dei dati personali (Decreto legislativo 30 giugno 2003, n. 196)non tuteli solo le persone fisiche ma anche le persone giuridiche, gli enti e le associazioni (art.4 comma 1 lett. b) ed i)).

Il minor peso attribuito ai diritti fondamentali della persona è visibile anche in altre disposizioni, quale ad esempio la norma sull'accesso abusivo, volta a proteggere sulla carta il diritto del singolo di vivere serenamente nel suo domicilio informatico, che, tuttavia, prevede degli aggravamenti di pena allorquando l'intrusione riguardi sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico.

Altro fattore da considerare è che la legislazione penale sulle tecnologie si distingue per l'impiego di un linguaggio "tecnico" sinora sconosciuto nell'ambito dell'ordinamento penale. Le nuove disposizioni si riferiscono a "sistemi informatici e telematici, a "parole chiave", a "misure di sicurezza", a "programmi informatici, senza mai spiegarne il significato.

Discorso a parte va fatto poi rispetto alle norme penali non espressamente riferite a condotte realizzabili attraverso le tecnologie dell'informazione, è il caso di delitti quali la diffamazione, estorsione, truffa, che essendo a forma libera possono essere realizzati con qualsiasi mezzo e quindi anche attraverso la rete. In ordine a queste ultime, infatti, il tratto distintivo risiede nel fatto che esse vanno adattate alle nuove fenomenologie attraverso processi interpretativi di aggiustamento.

Come tutto ciò possa influire nelle decisioni dei giudici lo dimostra la lettura di alcune sentenze, dalle quali traspaiono diversi "momenti di condizionamento", alcuni direttamente riconducibili al tenore letterale del disposto normativo, altri al contesto in cui la disposizione deve essere calata, altri ancora ad una visione personale delle tecnologie da parte dell'interprete.[21]

Allorquando la condotta non è espressamente regolamentata, il giudice può essere influenzato da valutazioni di carattere tecnico. Rispetto al delitto di violazione di corrispondenza, ad esempio, si può giungere a conclusioni differenti a seconda che si consideri la posta elettronica in tutto e per tutto uguale alla posta tradizionale ovvero si evidenzino eventuali differenze.[22]

---

[21] "Applicare una legge non è come risolvere un'equazione algebrica o altro problema di matematica, rispetto alla cui soluzione non v'è alternativa tra il risultato esatto, da un lato, e l'errore dall'altro (l'uno e l'altro egualmente incontrovertibili e dimostrabili matematicamente), non implica tanto una capacità di ragionare, quanto soprattutto una ricchezza di sentimento, perché è quest'ultima che ci guida nel costante sforzo di mantenere il diritto sul binario della Giustizia. Come affermava il Kirchman, le decisioni sulle questioni di diritto (cioè il modo di interpretare e coordinare le leggi)scaturiscono più dal cuore che dalla mente", così R.Borruso, *L'interpretazione della legge e l'informatica*, in R.Borruso, R.Maria Di Giorgi, L.Mattioli, M.Ragona, *L'informatica del diritto*, Giuffrè, Milano, 2004, p. 350.

[22] Cfr. ordinanza del 10 maggio 2002 del GIP di Milano, con la quale viene archiviato un procedimento aperto a seguito di denuncia-querela sporta da un dipendente nei confronti del responsabile del reparto e del legale rappresentante della società per violazione di corrispondenza. All'interno di tale provvedimento, infatti, si evidenziano le differenze tra posta tradizionale ed elettronica: "Né può ritenersi conferente ogni ulteriore argomentazione che, facendo apoditticamente leva sul carattere di assoluta assimilazione della posta elettronica alla posta tradizionale, cerchi di superare le strutturali diversità dei due strumenti comunicativi (si pensi, in via esemplificativa, al carattere di "istantaneità" della comunicazione informatica - operante come un normale terminale telefonico - pur in presenza di

Stesso discorso per quanto attiene al delitto di diffamazione via Internet, la cui consumazione si riterrà dimostrata con la semplice prova dell'invio del messaggio ove si consideri la rete strumento analogo ad altri media, ritenendosi, viceversa, necessaria ai medesimi fini la prova dell'avvenuta ricezione da parte di terzi nel caso in cui si reputi la rete mezzo diverso, rispetto al quale la lettura di un'informazione non può essere presunta.[23]

In che modo la " lettura " delle tecnologie possa influire sull'applicazione della norma viene dimostrato da una serie di decisioni in ordine alla rilevanza penale delle scommesse raccolte in Italia per via telematica e trasmesse con lo stesso mezzo a *bookmaker* presente in un Paese dove quella condotta è ritenuta legittima. Orbene, in ordine a tale materia, se alcune decisioni conferiscono alla rete il ruolo di un semplice mezzo di comunicazione, escludendo il delitto sull'assunto che il gestore dell'*internet point* si limita a consentire la stipulazione a distanza di un contratto di scommessa[24], altre ammettono la sussistenza del delitto reputando la trasmissione via rete condotta concorrente a quella posta in essere all'estero.[25]

Ulteriori problemi interpretativi possono, tuttavia, sorgere, quando il giudice è chiamato ad applicare norme espressamente riferite a condotte realizzate con le tecnologie dell'informazione. Prendendo, ad esempio, il delitto di accesso abusivo, che punisce l'intrusione all'interno di un sistema informatico o telematico protetto da misure di sicurezza, la sua sussistenza potrà essere affermata o negata anche a seconda del significato attribuito al termine "sistema" - non è, infatti, ancora pacifico se in tale concetto possa rientrare l'impianto televisivo satellitare[26] o il centralino telefonico[27], o all'espressione "misure di sicurezza".[28]

Altre questioni interpretative possono dipendere dalla genericità con la quale alcune nome fanno riferimento alle tecnologie. Di fronte alla disposizione che punisce la distribuzione per via

un prelievo necessariamente legato all'accensione del personal e, quindi, sostanzialmente coincidente con la presenza stanziale del lavoratore nell'ufficio ove è presente il *desk-top* del titolare dell'indirizzo) per giungere a conclusioni differenti da quelle ritenute da questo giudice".

[23] Cfr. sentenza 112/02 del Tribunale di Teramo ove si afferma che: " Né può affermarsi, è da aggiungere, che in tale caso sia possibile presumere la conoscenza del messaggio da parte di terzi, come potrebbe sostenersi nel caso della stampa o della diffusione televisiva ……Infatti del tutto diverso in questi casi è il mezzo di diffusione, rispetto al quale può ritenersi effettivamente ragionevole dare per provato che un giornale sia letto da più persone o una trasmissione televisiva raggiunga più spettatori. Peraltro quanto alla diffamazione a mezzo stampa va detto che una prima diffusione comunque già si realizza al momento della consegna da parte dello stampatore delle prescritte copie in adempimento dell'obbligo previsto dalla l. 2 Febbraio 1989 n 374, che ovviamente non ha riscontro nel caso in esame per le peculiarità del mezzo tecnico. Nella diffamazione a mezzo Internet quanto alla visibilità del messaggio va evidenziato che nessun sito può essere raggiunto per caso. E' necessario conoscerlo o quantomeno procedere ad una precisa interrogazione di un motore di ricerca. Il motore di ricerca è a sua volta un sito, all'interno del quale è possibile consultare degli elenchi, aggiornati periodicamente, che contengono delle brevi recensioni di ogni sito web e consentono di raggiungerlo grazie ad un collegamento ipertestuale."

[24] Cfr. Tribunale di Santa Maria Capua Vetere sentenza 14 luglio 2000; nella stessa direzione Tribunale di Siena sentenza 23 ottobre 2000.

[25] Cfr. Tribunale del Riesame di Palermo, ordinanza 19 giugno 2000.

[26] Cfr.Cass. Sez.VI n.4389/98;in senso contrario le argomentazioni proposte nella richiesta di archiviazione avanzata dalla Procura di Crotone(PM Torriello)in data 18 marzo 2002.

[27] Cfr. Cass. Sez.VI n.3067/99.

[28] Cfr. sentenza Tribunale di Torino 7 febbraio 1998 e Cass.Sez.V n.12732/00 secondo cui per la sussistenza del delitto basta qualunque misura di protezione, anche esterna; vedi anche sentenza del Tribunale di Roma del 4 aprile 200, Sez.VIII Gip Landi, secondo cui necessitano "mezzi efficaci di protezione".

telematica di materiale pedopornografico, intendendosi per tale la trasmissione ad un numero indeterminato di destinatari, l'invio all'interno di una *chat* potrà essere valutato diversamente a seconda della volontà e competenza del giudice di comprendere il funzionamento del servizio utilizzato e sottoposto alla sua attenzione.[29]

Differenti valutazioni possono, infine, dipendere dall'entroterra culturale dello stesso organo giudicante. Il giudice è un uomo ed in quanto tale soggetto con una propria visione del mondo ed inevitabilmente con un suo sentire politico. Piaccia o non piaccia la sua storia può influenzare le sue decisioni, e ciò sovente senza che lo stesso se ne accorga.

Emblematica in tal senso quella sentenza con la quale è stato assolto un extracomunitario sorpreso a vendere *compact disc* contraffatti, ritenendosi applicabile al caso di specie l'esimente dello stato di necessità e ciò dopo aver criticato apertamente i regimi di oligopolio esistenti e dopo aver rilevato le difficoltà di adattamento in una società siffatta.

Alla luce delle valutazioni svolte in ordine al rapporto intercorrente tra giudice, norma e contesto in cui la stessa va applicata, emerge un ulteriore ruolo delle tecnologie dell'informazione in ambito giuridico: le tecnologie quale "misuratore" della tenuta dell'ordinamento giuridico.

In un recente passato le tecnologie hanno messo in crisi il "mito" della completezza dell'ordinamento giuridico, imponendo la previsione di nuove regole adatte a regolamentare nuove realtà.

Oggi, che le norme ci sono, la tecnologia si pone come osservatorio dal quale guardare l'impatto effettivo delle nuove e vecchie norme, rilevandone le contraddizioni interne e quelle direttamente riconducibili ai differenti punti di vista degli organi giudicanti.

[29] Cfr. Cass. Sez. III n.5397/01.

Rivista elettronica di Diritto, Economia, Management

N. 1 - 2010 · pp. 116-127

La protezione dei dati personali nell'Unione Europea dopo il Trattato di Lisbona

Sandro Di Minco

Abstract: L'entrata in vigore del Trattato di Lisbona segna un passaggio molto rilevante anche in materia di *data protection* dando un impulso decisivo al processo di progressivo riconoscimento del diritto alla protezione dei dati personali in Europa, quale diritto fondamentale della persona. Si è conseguentemente delineato un nuovo contesto giuridico europeo che rende possibile, se non necessaria, la configurazione di un regime giuridico globale di protezione dei dati applicabile a tutte le operazioni di trattamento, in tutti gli ambiti di competenza dell'UE, costituito a partire dai principi chiave della Direttiva 95/46/CE, opportunamente adattati al nuovo contesto istituzionale e tecnologico. Tale regime globale, non esclude tuttavia l'adozione di norme supplementari specifiche sia per la protezione dei dati in ambito PESC, sia in relazioni alle necessità proprie dell'ambito della cooperazione giudiziaria e di polizia per fini di contrasto della criminalità. In ogni caso i trattamenti di dati personali sono soggetti al controllo di Autorità indipendenti di cui vanno rafforzati, chiariti e armonizzati funzioni e poteri oltre alla necessità di migliorarne la cooperazione ed il coordinamento.
Parole chiave: Trattato di Lisbona, protezione dei dati personali, Unione europea, Carta dei diritti fondamentali, Direttiva 95/46/CE, art. 16 TFUE, art. 39 TUE, Autorità indipendenti, Garante europeo, Decisione-quadro 2008/977/GAI, Regolamento n. 45/2001, regime giuridico globale, Programma di Stoccolma.

1. Trattato di Lisbona e tutela dei dati personali nell'UE

L'entrata in vigore del Trattato di Lisbona, aldilà di tutte le altre importanti ed ampie implicazioni, segna un passaggio molto rilevante anche sul piano del diritto alla privacy dando un impulso decisivo al processo, di progressivo riconoscimento del diritto alla tutela dei dati

Articolo pervenuto il 15 ottobre 2010, approvato il 1 dicembre 2010

personali in Europa quale diritto fondamentale della persona, avviato da oltre sessanta anni con la stipula della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU) del 1950.

Tra i primi effetti del Tr. Lisb. da segnalare, con implicazioni in materia di protezione dei dati personali, vi è senz'altro l'attribuzione dello stesso valore giuridico dei trattati alla Carta dei diritti fondamentali[1] ai sensi del nuovo art. 6 TUE.

Benché la stessa Corte di Giustizia e alcuni giudici nazionali avessero già basato diverse decisioni sulla stessa Carta di Nizza, sin dal 2000 - e in qualche caso ancor prima della sua formale "proclamazione"[2]- riconoscendole di fatto una "forza giuridica" superiore a quella che formalmente le era assegnata nella gerarchia delle fonti del diritto dell'UE - il riconoscimento di un così elevato valore giuridico formale attribuito alla Carta dei diritti fondamentali, rappresenta una forte novità non solo nel quadro generale dell'UE, ma anche con particolare riferimento al definitivo riconoscimento di un "fondamento costituzionale" al diritto alla protezione dei dati personali, in forza dell'art. 8 della Carta stessa.

Il contenuto del suddetto art. 8 - ai sensi del quale: *"1. Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano. 2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica. 3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente"* - rappresenta un'innovazione forte, anche perché la protezione dei dati è stata distinta dalla tutela tradizionale della privacy ed è stata formalmente riconosciuta quale diritto fondamentale autonomo. Un diritto fondamentale di cui l'art. 16 TFUE rappresenta una estensione nel Trattato sul funzionamento dell'Unione Europea.

Questa nuova situazione segna l'approdo di un lungo processo che, come detto, ha portato al livello più alto mai raggiunto nel riconoscimento del diritto alla protezione dei dati personali nell'Unione Europea.

Si è già fatto riferimento all'art. 16 TFUE – in base al cui contenuto *"1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. 2. Il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria, stabiliscono le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e degli organismi dell'Unione, nonché da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti. 3. Le norme adottate sulla base del presente articolo fanno salve le norme specifiche di cui all'articolo 39 del trattato sull'Unione europea"* - rispetto al quale appare opportuno effettuare di seguito alcune riflessioni.

A proposito della sua portata, considerando anche quanto accennato a proposito della Carta dei diritti, appare ragionevole sostenere che l'art. 16 TFUE - il cui testo ripropone pressoché letteralmente l'art. **I-51** del Trattato di Roma, (*Trattato che adotta una Costituzione per l'Europa*)

---

[1] Proclamata ufficialmente una prima volta a Nizza nel dicembre 2000 dal Parlamento europeo, dal Consiglio e dalla Commissione e successivamente adattata e nuovamente proclamata nel dicembre 2007.

[2] Emblematico il caso della sentenza del 30 novembre 2000 della Corte Costituzionale Spagnola che prima ancora della proclamazione ufficiale della Carta dei diritti fondamentali ha fatto riferimento al suo art. 8.

- vada dunque letto ed interpretato in maniera coordinata ed integrata con l'art. 8 della Carta dei diritti fondamentali, con la conseguenza di determinare un profondo mutamento, rispetto al passato, proprio nei valori di fondo che devono guidare le scelte normative del legislatore europeo, presenti e future, in tema di protezione dei dati personali nonché la stessa interpretazione, in sede applicativa, di quelle previgenti.

Ciò implica per il legislatore europeo, l'attuale "disponibilità" (ma anche i vincoli che ne conseguono) di una base giuridica specifica ed autonoma (proprio nell'art. 16 TFUE) su cui fondare eventuali atti normativi in materia di dati personali. Si ricorderà invece che il contesto giuridico complessivo nel quale agiva il legislatore comunitario negli anni 90 era diverso ed infatti il testo normativo di riferimento principale, a livello europeo, in materia di tutela dei dati – la direttiva 95/46/CE – sul piano giuridico formale aveva la sua base giuridica nell'art. 95 del TCE (precedentemente articolo100A) traendo la sua origine da motivi di mercato interno. In effetti l'adozione di un atto normativo specifico, a livello comunitario, veniva giustificata dall'esigenza di superare e comporre le differenze nell'atteggiamento adottato dagli Stati membri in materia e, dunque, al fine di eliminare un ostacolo alla libera circolazione dei dati personali tra gli Stati membri attraverso un intervento di armonizzazione.

Va però anche detto che il testo della Dir. 95/46 è stato in gran parte ispirato ai principi della Convenzione n. 108 di Strasburgo e, in effetti, esso affianca ad uno dei più tradizionali obiettivi del progetto di integrazione europea - il completamento del mercato interno (in questo caso, la libera circolazione delle informazioni personali) – anche la tutela dei diritti e delle libertà fondamentali dei cittadini. Nella Direttiva entrambi gli aspetti sono dichiarati quali obiettivi posti, teoricamente, sullo stesso piano anche se, come detto, in termini giuridico-formali la direttiva trae la sua origine da motivi di mercato interno.

La direttiva 95/46/CE è stata poi seguita da altri atti normativi europei[3] che hanno cercato di integrare il quadro normativo complessivo e di far fronte alle esigenze di protezione dei dati personali nei vari settori economico-sociali e dunque, in qualche caso, anche con riferimento ad attività ricadenti nell'ambito dei differenti Pilastri della costruzione europea (anche se, come noto, l'efficacia della Direttiva quadro, e dei principali altri atti normativi integrativi di questa, era limitata al solo ambito Comunitario con esclusione degli ex secondo e terzo pilastro).

---

[3] Il diritto comunitario derivato ha ulteriormente arricchito la normativa europea in materia, ad es. con un atto giuridico di settore, con la Direttiva *e-privacy* - Direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche) in GU, L 201 del 31 luglio 2002, p. 37 - che ha abrogato e sostituito, al fine di adeguarla meglio all'ambiente dell'Information Communication Technology, la precedente Direttiva 97/66/CE del Parlamento europeo e del Consiglio, del 15 dicembre 1997, "sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni" (GU L 24 del 30.1.1998, pag. 1), la quale, a sua volta, aveva "tradotto i principi enunciati dalla direttiva 95/46/CE in norme specifiche per il settore delle telecomunicazioni" (Dir. 2002/58, considerando 4). Altro atto giuridico di rilievo in materia è poi il Regolamento istitutivo del Garante europeo per la protezione dei dati - Regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati (GU L 008 del 12/01/2001 p.1) – e, più recentemente, la Decisione quadro 2008/977/GAI del 27 novembre 2008 sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale (GUE, L 350, del 30 dicembre 2008, p. 60).

Con particolare riferimento poi all'ambito della cooperazione giudiziaria e di polizia in materia penale, si richiama la Decisione quadro 2008/977/GAI del 27 novembre 2008 sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale, con la quale si è cercato di avere un approccio unitario, quantomeno in relazione a tutti i trattamenti effettuati nel suddetto ambito, anche se la disciplina citata non può essere considerata come l'avvenuta realizzazione di un quadro giuridico globale nell'Unione[4]
Da questi pochi e rapidi riferimenti appare evidente che la disciplina europea in materia di dati personali difetti di un approccio tendenzialmente unitario, ancor più necessario a seguito del richiamato superamento della rigida divisione in "Pilastri" della costruzione europea.

2. Verso un regime giuridico globale di protezione dei dati

Il Trattato sul funzionamento dell'Unione europea, con l'art. 16, come detto, ha creato una base giuridica comune che crea le condizioni per la realizzazione di un quadro globale in materia di protezione dei dati ed il superamento della tendenziale frammentazione che invece ha caratterizzato la situazione europea sino ad oggi.
Si è già fatto cenno sopra ai problemi di coerenza in materia di protezione dei dati che dunque, a seguito dell'entrata in vigore del Tr. Lisb., da un lato tendono ad apparire più evidenti (ad es. in conseguenza del superamento della divisione in Pilastri) e dall'altro appaiono di più agevole superamento proprio in forza del nuovo contesto normativo complessivo.
La stessa Commissione ha sostenuto che "Occorrerà istituire un regime completo di protezione: l'Unione dovrà garantire un'azione globale e rinnovata in materia di protezione dei dati dei cittadini all'interno dell'Unione e nell'ambito delle relazioni con i paesi terzi, e dovrà altresì prevedere e regolare le circostanze in cui i pubblici poteri, nell'esercizio delle loro funzioni, potranno eventualmente porre i necessari limiti all'applicazione delle suddette norme"[5]. Su tali considerazioni della Commissione è successivamente intervenuto anche il Garante europeo per la protezione dei dati personali, (in seguito: GEPD) dichiarando che "interpreta l'enfasi posta dalla Comunicazione su un regime globale di protezione dei dati come un'ambizione della Commissione di proporre un quadro giuridico che si applichi a tutte le operazioni di trattamento. Approva pienamente tale ambizione in quanto rafforza la coerenza del sistema, assicura certezza del diritto e, così facendo, migliora la protezione".[6]
Lo stesso Programma di Stoccolma, il documento che definisce le priorità dell'UE nel settore della Giustizia e degli Affari Interni per il periodo 2010-2014 - approvato dal Consiglio europeo l'11 Dicembre 2009 - ha dedicato uno specifico punto alla tutela dei diritti dei cittadini

---

[4] Cfr. Parere del Garante europeo della protezione dei dati sulla comunicazione della Commissione al Parlamento europeo e al Consiglio dal titolo «Uno spazio di libertà, sicurezza e giustizia al servizio dei cittadini», cit. punto 29.

[5] Cfr. Comunicazione della Commissione al Parlamento europeo e al Consiglio dal titolo «Uno spazio di libertà, sicurezza e giustizia al servizio dei cittadini» - COM (2009) 262 definitivo del 10 giugno 2009, punto 2.3.

[6] Cfr. Parere del Garante europeo della protezione dei dati sulla comunicazione della Commissione al Parlamento europeo e al Consiglio dal titolo «Uno spazio di libertà, sicurezza e giustizia al servizio dei cittadini», cit., punto 35.

nella società dell'informazione[7] sostenendo che "L'Unione deve pertanto far fronte alle sfide insite nello scambio crescente di dati personali, e all'esigenza di garantire la protezione della vita privata. L'Unione deve garantire una strategia globale in materia di protezione dei dati all'interno dell'UE e nell'ambito delle relazioni con i Paesi terzi. [...] Dovrà altresì prevedere e regolare le circostanze in cui sia giustificato l'intervento dei pubblici poteri nell'esercizio di tali diritti ed applicare al contempo i principi relativi alla protezione dei dati nella sfera privata." Il Programma esprime poi l'invito alla Commissione a "valutare il funzionamento dei vari strumenti concernenti la protezione dei dati e presentare, se del caso, iniziative complementari, legislative o meno, atte a preservare l'efficace applicazione dei succitati principi". Un invito che la Commissione ha già raccolto concretamente se è vero che, proprio al momento di chiudere il presente contributo, prendiamo atto della Comunicazione della Commissione europea dal titolo: "Un approccio globale alla protezione dei dati personali nell'Unione europea"[8], appena pubblicata, che delinea la strategia della Commissione nella direzione di quella "armonizzazione orizzontale" più volte richiamata, al fine di garantire la protezione dei dati personali in tutti i settori. In questo documento si annuncia motivatamente che nel 2011 la Commissione presenterà le sue proposte per un nuovo quadro giuridico generale sulla protezione dei dati che dovrà essere negoziato e adottato dal Parlamento europeo e dal Consiglio.[9]

Va tuttavia precisato che i concetti di "armonizzazione" e di "quadro giuridico globale" in materia di protezione dei dati non vanno interpretati in maniera rigida e assoluta, in quanto bisognerà opportunamente tener conto di situazioni e contesti peculiari che richiedono delle norme specifiche.

Da questo punto di vista vanno senz'altro ricordati i "distinguo" che lo stesso Tr. Lisb. Ha espressamente già previsto. Infatti si ricorda che una base giuridica parzialmente diversa è attribuita alla tutela dei dati in ambito PESC (nuovo art. 39 TUE) ed inoltre nella Dichiarazione n. 21 relativa alla protezione dei dati personali nel settore della cooperazione giudiziaria in materia penale e della cooperazione di polizia, si afferma che potrebbero "rivelarsi necessarie, in considerazione della specificità dei settori in questione, norme specifiche per la protezione dei dati personali e sulla circolazione di tali dati".

Ciò detto appare tuttavia evidente che l'Unione europea si sia già messa in cammino al fine di perseguire un più elevato livello di armonizzazione in materia di protezione dei dati personali. Da questo punto di vista si ritiene opportuno segnalare, nei successivi quattro paragrafi, alcuni ambiti prioritari di intervento.

---

7 Cfr. Programma di Stoccolma. Cit., punto 2.5 Proteggere i diritti dei cittadini nella società dell'informazione.

8 Comunicazione della Commissione al Parlamento europeo, al consiglio, al comitato economico e sociale europeo e al comitato delle Regioni. Un approccio globale alla protezione dei dati personali nell'Unione europea COM(2010) 609 definitivo, del 4 novembre 2010.

9 Cfr. Comunicazione della Commissione (...) Un approccio globale alla protezione dei dati personali nell'Unione europea, cit. Inoltre, sul punto, cfr. le dichiarazioni di Viviane Reding, Vicepresidente della Commissione europea, Commissaria per la giustizia, i diritti fondamentali e la cittadinanza: «La protezione dei dati personali è un diritto fondamentale (…) Per garantirlo abbiamo bisogno di norme chiare e coerenti sulla protezione dei dati. Dobbiamo inoltre aggiornare la nostra legislazione per adeguarla alle sfide poste dalle nuove tecnologie e dalla globalizzazione. L'anno prossimo la Commissione presenterà una proposta legislativa per rafforzare i diritti delle persone, eliminando allo stesso tempo la burocrazia allo scopo di assicurare la libera circolazione dei dati nel mercato unico».

2.1 Modifica della Direttiva 95/46/CE

In primo luogo appare sicuramente opportuno intervenire a parziale modifica della normativa quadro rappresentata dalla Dir. 95/46. Da questo punto di vista, anche alla luce di quanto emerso nel corso della consultazione lanciata dalla Commissione il 9 luglio 2009 sull'argomento, sembra condivisa la convinzione della validità di fondo dei principi in essa contenuti anche in relazione alle sfide della tecnologia e della globalizzazione, mentre si ritiene di dover piuttosto migliorare il livello di protezione dei dati personali attraverso una migliore applicazione dei principi stessi. Alcuni aspetti che richiedono probabilmente un adeguamento della Direttiva sono, quello di una "modernizzazione" che tenga conto dell'evoluzione nel frattempo intercorsa; una migliore precisazione delle modalità applicative di alcuni principi chiave quali il consenso e la trasparenza; l'introduzione di nuovi principi come quello della "privacy by design", in base al quale l'attenzione alla protezione dei dati personali viene presa in considerazione in maniera anticipata - sin dalla fase della progettazione degli strumenti elettronici potenzialmente idonei al trattamento – al fine di integrare in tutto il ciclo di vita delle tecnologie (dalla fase di progettazione iniziale allo sviluppo, uso e smaltimento finale) la protezione della riservatezza e dei dati personali.[10]

Il recentissimo documento elaborato dalla Commissione per "un approccio globale alla protezione dei dati personali nell'Unione"[11] evidenzia in maniera ampia e argomentata i punti rispetto ai quali l'UE intende intervenire, entro il 2011, con modifiche ed integrazioni all'impianto della Dir. quadro, con riferimento, ad es., all'obiettivo di rafforzare i diritti delle persone.

Per conseguire tale obiettivo si propone di limitare allo stretto necessario la raccolta e l'utilizzo dei dati personali (rafforzando il principio della minimizzazione dei dati) e migliorare la trasparenza per gli interessati.[12] A tal fine la Commissione dichiara di voler integrare nel quadro giuridico un principio generale di trasparenza del trattamento dei dati personali e introdurre obblighi specifici a carico dei responsabili del trattamento in merito al tipo di informazioni da trasmettere e alle modalità per farlo, anche in relazione ai minori.

Il rafforzamento dei diritti delle persone interessate dal trattamento dei propri dati, secondo la Commissione, richiede anche di migliorare le modalità per l'effettivo esercizio dei diritti di accesso, rettifica e cancellazione o blocco dei dati (ad esempio introducendo termini di risposta alle richieste degli interessati, consentendo l'esercizio dei diritti per via elettronica o stabilendo che il diritto di accesso debba essere di norma gratuito); nonché di chiarire il cosiddetto «diritto all'oblio". La Commissione propone poi di integrare i diritti degli

---

[10] Cfr. anche *Un'agenda digitale europea. Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato delle Regioni*, Bruxelles, 19.5.2010, COM(2010)245 definitivo

[11] Cfr. Comunicazione della Commissione (...) Un approccio globale alla protezione dei dati personali nell'Unione europea, cit.

[12] "La trasparenza è una condizione fondamentale per permettere alle persone di esercitare un controllo sui propri dati e per assicurare una protezione efficace dei dati personali. È pertanto essenziale che gli interessati ricevano informazioni corrette, chiare e trasparenti dai responsabili del trattamento in merito alle modalità di raccolta e di trattamento dei dati che li riguardano, a chi li raccoglie e li tratta, per quali motivi e per quanto tempo, nonché al diritto di accesso ai dati, di rettifica e cancellazione" Cfr. Comunicazione della Commissione (...) Un approccio globale alla protezione dei dati personali nell'Unione europea, cit., punto 2.1.2. "Migliorare la trasparenza per gli interessati".

interessati assicurando il diritto di «data portability», ovvero il diritto esplicito di cancellare i propri dati (ad esempio foto, cartelle mediche o elenchi di amici) da un'applicazione o un servizio e, se tecnicamente possibile, di trasferirli a un'altra applicazione o servizio, senza opposizione del responsabile del trattamento.
Altro obiettivo da perseguire attraverso l'annunciato intervento legislativo europeo, è quello di rafforzare la dimensione «mercato interno» riducendo gli oneri amministrativi per le imprese e assicurando condizioni di parità reale in quanto le differenze nell'attuazione delle norme di protezione dati dell'UE e la scarsa chiarezza sulle normative nazionali applicabili ostacolano la libera circolazione dei dati personali in tutta l'UE e fanno aumentare i costi.
Altrettanto importante viene poi ritenuto l'obiettivo di garantire un alto livello di protezione per i dati trasferiti al di fuori dell'UE grazie a procedure migliori e semplificate per i trasferimenti internazionali di dati.
Il documento, come detto, è molto articolato ed argomentato, pertanto si rinvia direttamente al suo contenuto per una più completa visione dell'approccio che la Commissione intende adottare nella redazione della annunciata proposta di un atto legislativo entro il 2011.

2.2 Modifica della Decisione-quadro 2008/977/GAI

In secondo luogo appare pure opportuna una modifica della normativa specifica adottata con la Decisione quadro 2008/977 sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale in quanto molte delle sue disposizioni essenziali non sono in linea con la Dir. 95/46. Non si può ignorare che oggi i due provvedimenti, abbiano, come detto, una medesima base giuridica nell'art. 16 TFUE. Si ricorda che la Decisione quadro si applica in particolare ai dati trattati dalle autorità di polizia, doganali e giudiziarie ai fini della prevenzione, dell'indagine, dell'accertamento o del perseguimento dei reati o dell'esecuzione delle sanzioni penali. La disciplina in essa prevista riprende i principi generali di legalità, proporzionalità, finalità ed esattezza, nonché i diritti della persona interessata previsti dalla Convenzione di Strasburgo del 28 gennaio 1981.
Tanto la dottrina quanto altri interpreti ed organismi istituzionali – quali il Garante Europeo, il Gruppo di Lavoro Articolo 29, il Gruppo di lavoro Polizia e Giustizia[13] hanno analizzato alcuni aspetti problematici del contenuto della Decisione quadro, specie in relazione alla Direttiva quadro, evidenziando, ad es., il ristretto ambito applicativo di questa, limitato ai soli dati oggetto di trasmissione e scambio tra Stati membri, con esclusione dei dati trattati in ambito nazionale[14]; oppure le differenze nella disciplina riguardante il trattamento dei dati sensibili che nella Decisione quadro si basa sulle previsioni dell'art. 6, diverse da quelle dell'art. 8 della Direttiva; o ancora le differenze nel regime del diritto di accesso ai dati da parte della

[13] Creato dalla Conferenza delle Autorità europee incaricate della protezione dei dati, con il compito di controllare ed esaminare i progressi compiuti nel campo di polizia e della lotta alla criminalità a fronte delle sfide poste dalla protezione dei dati di carattere personale.

[14] Cfr. considerando 7, in base al quale "L'ambito di applicazione della presente decisione quadro si limita al trattamento dei dati personali trasmessi o resi disponibili tra Stati membri"

persona interessata come pure quelle riguardanti il trasferimento di dati a Stati terzi; nonché la mancata previsione di un "raccordo fra le Autorità nazionali di protezione dati e le autorità di controllo europee"[15], di cui è stata evidenziata la necessità di una istituzionalizzazione anche dal Garante europeo, dal Gruppo di Lavoro Articolo 29 Gruppo di Lavoro di Polizia e Giustizia[16]

Il Garante europeo ha dunque sostenuto l'opportunità, se non la necessità, di una modifica della citata Decisione che - in forza della nuova base giuridica rappresentata dall'art. 16 TFUE – porti ad un ampliamento del proprio ambito applicativo e ad un riallineamento con la Dir. 95/46[17]. Ferma restando, naturalmente, la possibilità di prevedere comunque norme specifiche per ambiti e situazioni peculiari, conformemente alle espresse previsioni della citata Dichiarazione n. 21; senza che tali deroghe impediscano comunque la configurazione di un regime minimo applicabile a tutti i tipi di trattamento, in qualsiasi ambito.

In maniera del tutto coerente con le sintetiche considerazioni appena svolte anche la Commissione ha recentissimamente posto tra gli obiettivi chiave dell'approccio globale alla protezione dei dati, proprio la revisione delle norme di protezione dei dati nell'ambito de,lla cooperazione polizia e giudiziaria in materia penale.

Tra i vari aspetti suscettibili di un intervento normativo la Commissione pone, ad es., la possibilità di "estendere l'applicazione delle norme generali di protezione dei dati ai settori della cooperazione di polizia e giudiziaria in materia penale, anche per il trattamento a livello nazionale, prevedendo se del caso limitazioni armonizzate di alcuni diritti riguardanti la protezione dei dati, ad esempio il diritto di accesso o il principio di trasparenza"[18]

---

[15] Cfr. In tal senso PIZZETTI, F., *La privacy come diritto fondamentale alla protezione dei dati personali nel Trattato di Lisbona,* in (a cura di) BILANCIA, P., D'AMICO, M., *La nuova Europa dopo il Trattato di Lisbona*, Milano, 2009, pag. 92, il quale evidenzia l'importanza del suddetto raccordo "tale da assicurare l'applicazione armonizzata delle disposizioni rilevanti in materia anche nell'ambito del Terzo Pilastro, con particolare riferimento alla valutazione dell'adeguato livello di protezione dati in vista di trasferimenti a Paesi terzi non europei" .

[16] Cfr. Groupe de travail «Article 29» sur la protection des données - Groupe de travail «Police et justice» 02356/09/FR, L'avenir de la protection de la vie privée - Contribution conjointe à la consultation de la Commission européenne sur le cadre juridique du droit fondamental à la protection des données à caractère personnel - 1 dicembre 2009, in particolare § 116

[17] Cfr. in tal senso Parere del Garante europeo della protezione dei dati sulla comunicazione della Commissione al Parlamento europeo e al Consiglio dal titolo «Uno spazio di libertà, sicurezza e giustizia al servizio dei cittadini», cit. punto 30

[18] Cfr. Comunicazione della Commissione (...) Un approccio globale alla protezione dei dati personali nell'Unione europea, cit., punto 2.3. "Rivedere le norme di protezione dei dati nell'ambito della cooperazione di polizia e giudiziaria in materia penale", pag. 16, dove la Commissione evidenzia anche i seguenti altri punti che si propone di esaminare per un intervento normativo di modifica e armonizzazione orizzontale: "- esaminare se il nuovo quadro giuridico generale sulla protezione dei dati debba contenere disposizioni specifiche e armonizzate, riguardanti ad esempio il trattamento dei dati genetici a fini penali o la distinzione tra le diverse categorie di persone interessate (testimoni, indiziati, ecc.) nel settore della cooperazione di polizia e giudiziaria in materia penale; - avviare nel 2011 una consultazione di tutte le parti interessate sul metodo migliore per revisionare gli attuali sistemi di controllo nei settori della cooperazione di polizia e giudiziaria in materia penale, al fine di garantire un controllo reale e coerente della protezione dei dati in tutte le istituzioni, organi, organismi e agenzie dell'Unione; - valutare la necessità di allineare, a lungo termine, le numerose norme settoriali vigenti adottate a livello dell'UE per la cooperazione di polizia e giudiziaria in materia penale nell'ambito di strumenti specifici, al nuovo quadro giuridico generale sulla protezione dei dati."

2.3 Una disciplina specifica in ambito PESC ai sensi dell'art 39 TUE

In terzo luogo, sicuramente l'entrata in vigore del Tr. Lisb. implica la necessaria adozione di un atto normativo specifico per la protezione dei dati in ambito PESC sulla base dell'art. 39 TUE. Il contenuto di tale articolo - in base al quale *"Conformemente all'articolo 16 del trattato sul funzionamento dell'Unione europea e in deroga al paragrafo 2 di detto articolo, il Consiglio adotta una decisione che stabilisce le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del presente capo, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti"* - evidenzia che la protezione dei dati di natura personale, quale diritto fondamentale della persona, grazie al Tr. Lisb. si estende oggi, a differenza che in passato, a tutti i settori di competenza dell'Unione europea, incluso quello della Politica estera e della sicurezza comune. Il Consiglio dovrà dunque necessariamente adottare un specifico atto normativo, più precisamente una Decisione, che disciplini il trattamento dei dati di carattere personale da parte degli Stati membri nell'esercizio di attività che rientrano nel settore della Politica estera e della Sicurezza comune nonché le norme relative alla libera circolazione di tali dati. Un disciplina giuridica che dovrà anche stabilire, obbligatoriamente, le modalità attraverso le quali il rispetto della normativa stessa sia sottoposta al controllo di Autorità indipendenti.[19]

Il contenuto dell'art. 39 TUE, come precisa testualmente lo stesso articolo, è sostanzialmente conforme a quello dell'art. 16 TFUE, rispetto al quale si può dunque rilevare un unico punto di discontinuità rappresentato dal differente strumento normativo prescelto per l'introduzione della disciplina stessa che, lo ricordiamo, in luogo della procedura legislativa ordinaria utilizza lo strumento normativo della Decisione, proprio dell'ambito della Politica estera e della sicurezza comune.

[19] Si ricorda, tra l'altro, che si tratta di uno dei 72 casi in cui è richiesta l'unanimità in seno al Consiglio e a tale riguardo si segnala la nota critica del Parlamento europeo, a proposito dei meccanismi di voto del Consiglio nel Trattato di Lisbona, secondo la quale "In tale materia il nuovo trattato ha praticamente seguito tutte le modifiche previste nella Costituzione. Le sole eccezioni riguardano il trattato di adesione alla Convenzione europea dei diritti dell'uomo, che dovrà essere approvata all'unanimità (QMV secondo la Costituzione) e la creazione di una nuova base giuridica relativa all'introduzione di norme sul trattamento dei dati personali nel quadro della PESC (articolo 39 TUE). Sebbene, secondo la migliore interpretazione, si tratti unicamente di stabilire regole comuni per l'esercizio di una competenza spettante in toto agli Stati membri (tutto ciò che riguarda le competenze dell'Unione in materia di protezione dei dati è soggetto all'articolo 16 TFUE), non ci si può che rammaricare del fatto che il Parlamento non sia stato associato a tale procedura e che non vi sia alcun riferimento esplicito al controllo da parte della Corte di giustizia", Cfr. Motivazione della Proposta di Risoluzione del Parlamento europeo sul Trattato di Lisbona (2007/2286(INI), nota 29.

2.4 Modifica del Regolamento n. 45/2001

Un breve richiamo sembra opportuno anche con riferimento al Regolamento n. 45/2001[20], che a seguito dell'entrata in vigore del Tr. Lisb., dovrà opportunamente essere modificato e/o integrato. Il suddetto Regolamento, ha la sua base giuridica nel precedente art. 286 TCE, introdotto dal Tr. Amsterdam, il quale prevedeva che *"A decorrere dal 1o gennaio 1999 gli atti comunitari sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati si applicano alle istituzioni e agli organismi istituiti dal presente trattato o sulla base del medesimo"*. Ed inoltre che *"il Consiglio* (...) *istituisce un organo di controllo indipendente incaricato di sorvegliare l'applicazione di detti atti alle istituzioni e agli organismi comunitari e adotta, se del caso, tutte le altre pertinenti disposizioni"*.

Sulla base di tale previsione fu pertanto adottato il citato "regolamento per accordare alle persone fisiche diritti giuridicamente tutelati e per chiarire gli obblighi dei responsabili del trattamento dei dati in seno alle istituzioni e agli organismi comunitari, nonché per istituire un'autorità di controllo indipendente incaricata di sorvegliare il trattamento dei dati personali effettuato dalle istituzioni e dagli organismi comunitari"[21]

Risulta dunque evidente la precisa delimitazione - al solo ambito comunitario - del campo di applicazione del Reg. n. 45/2001, nel contesto di una costruzione europea, articolata in pilastri, nettamente superata dal Tr. Lisb.

Come noto con il Reg. è stato istituito il GEPD che, come autorità indipendente, ai sensi dell'articolo 41, ha il compito di garantire il rispetto dei diritti e delle libertà fondamentali delle persone fisiche, segnatamente del diritto alla vita privata, da parte delle istituzioni e degli organismi comunitari nel trattamento dei dati personali. Il considerando 17 del regolamento, delinea la prospettiva nella quale il GEPD deve esercitare le proprie funzioni affermando che: "L'efficacia della tutela delle persone in relazione al trattamento dei dati personali nell'Unione presuppone la coerenza delle norme e delle procedure applicabili in materia ad attività inserite in quadri giuridici diversi."

Inoltre si ricorda anche che il considerando 16 del Reg. precisa che i compiti di sorveglianza del GEPD non si applicano ad organismi istituiti al di fuori dell'ambito comunitario, quali gli organismi istituiti nell'ambito del terzo pilastro del trattato UE.

Le sintetiche considerazioni appena svolte evidenziano l'esigenza, sopra richiamata, di armonizzare il ruolo e le funzioni del Garante europeo in relazione al nuovo quadro istituzionale.[22] A conferma della fondatezza di tale esigenza, la Commissione ha espressamente manifestato l'intenzione di procedere a valutare "se occorra adeguare altri atti legislativi al nuovo quadro giuridico generale. Sarà interessato anzitutto il regolamento (CE) n. 45/2001, di cui bisognerà adattare le disposizioni."[23]

---

[20] Regolamento (CE) n. 45/2001, cit.

[21] Cfr. Regolamento (CE) n. 45/2001, cit., considerando n. 5

[22] cfr. in tal senso PIZZETTI, F., *La privacy come diritto fondamentale alla protezione dei dati personali nel Trattato di Lisbona*, in (a cura di) BILANCIA, P., D'AMICO, M., *La nuova Europa dopo il Trattato di Lisbona*, Milano, 2009, pag. 96, testo e nota 21

[23] Comunicazione della Commissione (...) Un approccio globale alla protezione dei dati personali nell'Unione europea,

3. Brevi considerazioni conclusive

Dalle riflessioni sin qui svolte si evince che l'entrata in vigore del Tr. Lisb. ha determinato una importante evoluzione in materia di *data protection* conferendo al diritto fondamentale di ciascuno alla piena protezione dei dati personali, sia all'interno che all'esterno dell'UE, il riconoscimento più alto mai raggiunto in Europa.

Il contesto normativo attuale risulta nettamente più favorevole verso tale obiettivo, sia grazie al carattere giuridicamente vincolante riconosciuto alla Carta dei diritti fondamentali dell'Unione europea, il cui articolo 8 riconosce il diritto alla protezione dei dati personali, sia in virtù di una nuova base giuridica, nell'art. 16 TFUE, che consente di stabilire norme dell'Unione sistematiche e coerenti di protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale e alla libera circolazione di tali dati. "In particolare, la nuova base giuridica consente all'UE di disporre di un unico strumento giuridico per disciplinare la protezione dei dati, e ciò anche nei settori della cooperazione di polizia e della cooperazione giudiziaria in materia penale. L'ambito della politica estera e di sicurezza comune è solo parzialmente coperto dall'articolo 16 del TFUE, poiché a stabilire le norme relative al trattamento dei dati da parte degli Stati membri deve essere una decisione del Consiglio che si fonda su un'altra base giuridica"[24] (nell'art. 39 TUE).

Il controllo indipendente, già sancito dall'articolo 286 TCE - in riferimento dunque al solo ambito comunitario - e confermato quale principio generale nell'articolo 8, paragrafo 3 della Carta dei diritti fondamentali dell'Unione europea, viene ad essere ribadito espressamente nell'art. 16 TFUE nonché nell'art. 39 TUE e si configura quale requisito fondamentale per la protezione effettiva dei dati di carattere personale che dunque perviene ad essere "costituzionalizzato" con riferimento a tutti i settori di competenza dell'Unione, compreso quello della Politica estera e sicurezza comune.

La realizzazione di un "regime globale di protezione dei dati" è dunque possibile e necessaria. Esso dovrà verosimilmente basarsi su un nucleo minimo di norme, comune a tutti i tipi di trattamento, applicabile a tutti gli ambiti di competenza dell'Unione europea, costituito a partire dai principi chiave della Direttiva 95/46, opportunamente adattati al nuovo contesto istituzionale e tecnologico sulla base delle indicazioni fornite da ultimo dalla Commissione.[25] Tale regime minimo globale, come detto, non esclude l'adozione di norme supplementari specifiche sia per la protezione dei dati in ambito PESC, da adottare nei modi previsti dall'art. 39 TUE, sia che tengano conto delle necessità specifiche a fini di contrasto della criminalità, come previsto dalla Dichiarazione n. 21 allegata al Tr. Lisb., con riferimento all'ambito della cooperazione giudiziaria e di polizia. Infine, non si può ignorare che il tema del trattamento dei dati personali impone inevitabilmente un'ottica globale, e su questo aspetto vanno registrate con interesse le considerazioni contenute, sia nel Programma di Stoccolma, secondo il quale:

cit. Pag. 21

[24] Cfr. Comunicazione della Commissione (...) Un approccio globale alla protezione dei dati personali nell'Unione europea, cit., pag. 5.

[25] Cfr. Comunicazione della Commissione (...) Un approccio globale alla protezione dei dati personali nell'Unione europea, cit.

"l'Unione dovrà avere una funzione motrice per lo sviluppo e la promozione di **norme internazionali** in materia di protezione dei dati personali e la conclusione di adeguati accordi internazionali, tanto bilaterali che multilaterali",[26]sia nella recentissima Comunicazione della Commissione europea, in cui essa ribadisce la propria volontà di "- continuare a promuovere lo sviluppo di elevate norme di protezione dei dati, sia tecniche che giuridiche, nei paesi terzi e a livello internazionale; - impegnarsi a favore del principio della reciprocità della protezione nelle azioni internazionali dell'Unione e soprattutto nei confronti delle persone i cui dati sono esportati dall'UE verso paesi terzi; - rafforzare a tal fine la cooperazione con i paesi terzi e le organizzazioni internazionali come l'OCSE, il Consiglio d'Europa, le Nazioni Unite e altre organizzazioni regionali; - seguire da vicino lo sviluppo delle norme tecniche internazionali messe a punto dagli organismi di normazione come il CEN e l'ISO, per sincerarsi che integrino proficuamente le norme giuridiche e assicurino il rispetto effettivo sul piano operativo dei requisiti fondamentali di protezione dei dati."[27]

BIBLIOGRAFIA: WARREN, S. D., BRANDEIS, L. D., *The Right to privacy*, in Harvard Law review, 1890, 4, 193; WESTIN, A. F., *Privacy and freedom*, Atheneum, New York, 1967; FRIED, C., *Privacy*, in Yale L. J., 1968, 77, 475; MILLER, A. R., *Personal privacy in the computer age: the challenge of a new technology in an information-oriented society*, in Mich. L. Rev., 1969, 67, 1091; RODOTÀ, S., *Elaboratori elettronici e controllo sociale*, Bologna, 1973; ID., *Tecnologie e diritti*, Bologna 1995; ID., CONTI, P. (a cura di), *Intervista su Privacy e libertà*, Roma – Bari, 2005; ID., *La vita e le regole*, Milano, 2006; ALPA, G., *Raccolta di informazioni, protezione dei dati e controllo degli elaboratori elettronici (in margine ad un progetto di Convenzione del Consiglio d'Europa*), in Foro it., 1981, V, 27; BUTTARELLI, G., *Banche dati e tutela della riservatezza*, Milano, 1997; CUFFARO, RICCIUTO, ZENO-ZENCOVICH, (a cura di) *Trattamento dei dati e tutela della persona*, Milano, 1998; FROSINI, V., *Informatica, diritto e società*, Milano, 1998; PARDOLESI, R. (a cura di) *Diritto alla riservatezza e circolazione dei dati personali*, Milano, 2003; PECORA, L., STAGLIANÓ, G., *Massimario 1997 – 2001. I principi affermati dal Garante nei primi cinque anni di attività*, Roma, 2003; UBERTAZZI, T. M., *Il diritto alla privacy. Natura e funzione giuridiche*, Padova, 2004; DUMORTIER, F., POULLET, Y., *La protection des données à caractère personnel dans le contexte de la construction en piliers de l'Union Européenne*, Namur, 2006; PAISSAN, M., (a cura di) *Privacy e giornalismo. Diritto di cronaca e diritti dei cittadini* (2 ed.), Roma, 2006; PIZZETTI, F., *La privacy come diritto fondamentale alla protezione dei dati personali nel Trattato di Lisbona,* in (a cura di) BILANCIA, P., D'AMICO, M., *La nuova Europa dopo il Trattato di Lisbona*, Milano, 2009, 83-97; VIVANT, M. (diretto da) *Lamy Droit de l'Informatique et des Réseaux, Paris*, 2010; DI MINCO, S., *Commento all'art. 16 del TFUE* in (a cura di) CURTI GIALDINO, C., *Commentario al Trattato sull'Unione europea e al Trattato sul funzionamento dell'Unione Europea dopo Lisbona*, Napoli, (in corso di pubblicazione – Gennaio 2011).

[26] Cfr. Programma di Stoccolma, cit., punto 2.5 *Proteggere i diritti dei cittadini nella società dell'informazione*.

[27] Cfr. Comunicazione della Commissione (...) Un approccio globale alla protezione dei dati personali nell'Unione europea, cit., punto 2.4. *La dimensione globale della protezione dei dati*

Rivista elettronica di Diritto, Economia, Management

N. 1 - 2010 · pp. 128-136

Il procedimento amministrativo informatico

Wanda D'Avanzo

Abstract: L'*e-government* rappresenta, oggi, uno degli elementi principali dell'*iter* riformatore che interessa la pubblica amministrazione. L'innovazione passa attraverso l'applicazione delle nuove tecnologie informatiche e telematiche ai tradizionali istituti amministrativi portando ad un ripensamento delle procedure nel loro insieme. Ripensamento che è in rado potenzialmente di apportare un ammodernamento radicale della pubblica amministrazione, aumentandone la funzionalità.

Parole chiave: digitalizzazione, *e-government*, codice dell'amministrazione digitale, protocollo informatico, fascicolo informatico, sistema pubblico di connettività, documento informatico, firma digitale, posta elettronica certificata.

1. Introduzione

Con il termine *e-government* (governo elettronico) s'intende l'utilizzo delle moderne tecnologie dell'informazione e della comunicazione nel processo di ammodernamento della pubblica amministrazione, che comprende tre principali categorie di azioni: "quelle di informatizzazione, dirette a migliorare l'efficienza operativa interna delle singole amministrazioni; quelle dirette ad informatizzare l'erogazione dei servizi ai cittadini e alle imprese implicanti una integrazione tra i servizi delle varie amministrazioni; infine, quelle dirette a consentire l'accesso telematico degli utilizzatori finali ai servizi della PA e alle sue informazioni"[1]. Il disegno d'innovazione

[1] M. Perin, *Internet e semplificazione amministrativa*, in G. Cassano (a cura di), *Diritto delle nuove tecnologie e dell'Internet*, Ipsoa, Milano, 2002, p. 1268. Per una disamina più approfondita delle problematiche di *e-government* e una descrizione analitica del procedimento amministrativo informatico mi sia consentito un rinvio al mio W. D'Avanzo, *L'e-government*, Movimedia, Lecce, 2007.

Articolo pervenuto il 15 ottobre 2010, approvato il 1 dicembre 2010

passa attraverso "l'abbandono del modello di sistema informativo pubblico centralizzato […], per realizzare, invece, architetture basate sulla condivisione delle informazioni e sulla cooperazione applicativa fra i sistemi pubblici e privati, pervenendo a soluzioni che consentano ai cittadini e alle imprese di entrare in contatto con le amministrazioni partendo da un punto qualsiasi della rete delle PA e di accedere ai servizi pubblici utilizzando i propri terminali […]"[2].

La principale disposizione normativa che ha reso possibile l'ingresso, nelle amministrazioni italiane, degli strumenti tecnico-informatici è stata la legge 15 marzo 1997, n. 59, nota anche come legge Bassanini, in cui è contenuta la disposizione secondo la quale "gli atti, dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge. I criteri e le modalità di applicazione del presente comma sono stabiliti per la pubblica amministrazione e per i privati, con specifici regolamenti da emanare entro centosettanta giorni dalla entrata in vigore della presente legge […]" (art. 15, comma 2).

Da allora, il complesso meccanismo di riforma delle istanze procedurali del settore pubblico, che, così, ha iniziato a delinearsi, ha proseguito nella sua evoluzione, nell'ottica di una sempre maggiore semplificazione e il 7 marzo 2005 è stato emanato il d.lgs. n. 82, recante codice dell'amministrazione digitale, il cui scopo è stato quello di rendere obbligatoria l'innovazione della PA offrendo, da una parte, ai cittadini e alle imprese nuovi diritti di partecipazione telematica a tutte le pubbliche attività; dall'altra, stabilendo che tutte le amministrazioni debbano organizzarsi in modo da rendere sempre disponibili le informazioni da esse possedute in forma digitale. Una prima modifica al codice è intervenuta con d.lgs. 159/2006.

2. I fondamenti della digitalizzazione. Nuovi diritti e principi di organizzazione

Nei primi articoli, il codice dell'amministrazione digitale del 2005 individua e disciplina i nuovi diritti dei cittadini e delle imprese nei confronti delle pubbliche amministrazioni, attuabili grazie all'uso delle tecnologie dell'informazione e della comunicazione, oltre che i principi di riorganizzazione in funzione della digitalizzazione della pubblica amministrazione. I principali nuovi diritti dei cittadini nei confronti dell'amministrazione sono il diritto all'uso delle tecnologie per tutti i rapporti con qualsiasi amministrazione dello Stato (art. 3); il diritto all'accesso telematico ai documenti amministrativi e all'invio di documenti digitali (art. 4); il diritto a effettuare qualsiasi pagamento in forma digitale (art. 5); il diritto a ricevere qualsiasi comunicazione pubblica tramite posta elettronica (art. 6); il diritto alla qualità del servizio (art. 7).

Le PA, d'altro canto, nell'organizzare autonomamente la propria attività, devono utilizzare le tecnologie dell'informazione e della comunicazione, al fine di realizzare gli obiettivi di

[2] C. Silvestro, *E-government, e-governance, e-democracy*, in G. Cassano (a cura di), cit., p. 1247.

efficienza, efficacia, economicità, imparzialità, trasparenza, semplificazione e partecipazione, garantendo, nel rispetto delle vigenti normative, l'accesso alla consultazione, la circolazione e lo scambio di dati e informazioni, nonché l'interoperabilità dei sistemi e l'integrazione dei processi di servizio fra le diverse amministrazioni (art. 12).
La riorganizzazione strutturale e gestionale delle pubbliche amministrazioni, attraverso l'utilizzo delle tecnologie dell'informazione e della comunicazione, ai sensi dell'art. 15 del codice, deve avvenire con la razionalizzazione e semplificazione dei procedimenti amministrativi, delle attività gestionali, dei documenti, della modulistica, delle modalità di accesso e di presentazione delle istanze da parte dei cittadini e delle imprese. Lo Stato, per parte sua, ha il compito di promuove la realizzazione e l'utilizzo di reti telematiche come strumento d'interazione tra le pubbliche amministrazioni ed i privati.

3. La firma digitale

Per dare concreta attuazione alla completa dematerializzazione del patrimonio informativo della PA e all'automazione delle varie fasi in cui si articolano i procedimenti amministrativi, fondamentale importanza rivestono la firma digitale e la posta elettronica certificata, che consentono, rispettivamente, di attribuire validità a tutti gli effetti di legge al documento informatico e di consentirne l'invio o la ricezione tramite le nuove tecnologie.
Il documento informatico è la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti. La firma digitale è "un particolare tipo di firma elettronica qualificata basata 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 del documento informatico o di un insieme di documenti informatici" (art. 1, d.lgs. 82/2005).
La chiave privata, nel sistema di firma digitale, è conosciuta dal solo soggetto titolare e l'algoritmo che la genera è contenuto in un dispositivo di *smartcard*. La corrispondente chiave pubblica consente la verifica della sottoscrizione apposta al documento informatico dal titolare della firma. La chiave pubblica è depositata nella banca dati del certificatore che è il soggetto, pubblico o privato, che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime.
Il documento informatico sottoscritto con firma digitale garantisce l'identificabilità dell'autore, l'integrità e l'immodificabilità del documento, si presume riconducibile al titolare del dispositivo di firma e soddisfa comunque il requisito della forma scritta; fa, dunque, piena prova, fino a querela di falso, della provenienza delle dichiarazioni di chi lo ha sottoscritto. L'apposizione della firma digitale, inoltre, integra e sostituisce l'apposizione di sigilli, timbri, contrassegni di qualsiasi genere. La firma digitale apposta su un documento informatico equivale, pertanto, alla sottoscrizione autografa apposta su un documento cartaceo[3].

[3] G. Finocchiaro, *La firma digitale. Formazione, archiviazione e trasmissione di documenti con strumenti informatici e telematici*, in F. Galgano (a cura di), *Commentario al codice civile Scialoja-Branca, art. 2699-2720, supplemento (d.p.r. 10 novembre 1997,*

4. La posta elettronica certificata (PEC)

I documenti informatici, le copie, gli estratti possono essere trasmessi con qualsiasi mezzo informatico o telematico, idoneo ad accertarne la provenienza. La trasmissione informatica del documento soddisfa il requisito della forma scritta ed esonera da ogni obbligo di produzione ed esibizione del documento cartaceo (art. 45, comma 1, d.lgs. 82/2005).
Analogamente, "le comunicazioni tra le pubbliche amministrazioni, avvengono di norma mediante l'utilizzo della posta elettronica; esse sono valide ai fini del procedimento amministrativo una volta che ne sia verificata la provenienza" (art. 47, comma 1).
Nel contesto della riforma digitale della pubblica amministrazione, dunque, particolare rilievo assumono le norme in materia di posta elettronica. A partire dal riferimento primario costituito dall'articolo 15, comma 2, della l. 15 marzo 1997, n. 59, il quadro normativo di riferimento è costituito principalmente dal d.p.r. 11 febbraio 2005, n. 68, contenente disposizioni per l'utilizzo della posta elettronica certificata (PEC).
Il d.p.r. 68/05 ha confermato il concetto della validità giuridica della trasmissione del documento informatico, e ne ha disciplinato le modalità di trasmissione e l'interoperabilità, la ricevuta di accettazione di avvenuta consegna, la ricevuta di presa in carico e l'avviso di mancata consegna, la sicurezza della trasmissione[4].
La PEC è un sistema di posta elettronica che si caratterizza per il fatto di poter essere utilizzata in qualsiasi contesto ove sia necessario avere la prova opponibile dell'invio e della consegna dei documenti. Attraverso l'impiego della posta elettronica certificata, infatti, nei casi d'invio e ricezione telematica di documenti informatici, è possibile la conoscibilità certa della casella di posta mittente. Inoltre, alla casella di posta elettronica è associata una particolare funzione che permette il rilascio delle ricevute di avvenuta consegna al ricevimento della corrispondenza. L'invio di documenti informatici tramite PEC, come nel caso di documenti cartacei spediti tramite raccomandata A/R nel sistema di posta ordinario, soddisfa le trasmissioni che necessitano delle ricevute di invio e di consegna, con opponibilità ai terzi delle relative attestazioni temporali.

5. Il procedimento amministrativo informatico

Nella prospettiva del codice dell'amministrazione digitale, le pubbliche amministrazioni redigono gli originali dei propri documenti con strumenti informatici. La formazione dei documenti in maniera digitale è, dunque, il primo passo per la compiuta dematerializzazione del patrimonio informativo raccolto e prodotto dalla PA nei registri e negli archivi pubblici, su cui poggia la concreta possibilità di addivenire ai momenti successivi di gestione elettronica dei flussi documentali, e, conseguentemente, anche dei procedimenti amministrativi, e di conservazione delle informazioni con modalità digitali.

n. 513), Bologna, 2000, p. 1.

4 D.A. Limone, *Codice dell'amministrazione digitale: pro e contro*, in *E-Gov*, IV, 6, 2005, p. 19.

La gestione dei flussi documentali, scambiati all'interno ed all'esterno dell'organizzazione pubblica, nonché la gestione dei procedimenti amministrativi con l'ausilio delle tecnologie ICT, sono rese possibili dagli applicativi di protocollo informatico e dalla possibilità di creare fascicoli informatici per i singoli procedimenti e, tramite le strutture di cooperazione applicativa, consentono il dialogo diretto tra i sistemi informativi degli enti. Ed, invero, nel sistema di gestione dei flussi documentali, la classificazione dei documenti informatici assume rilievo fondamentale anche al fine di garantire l'archiviazione e la successiva conservazione digitale, quale processo finalizzato a rendere un documento non deteriorabile e, quindi, facilmente reperibile nel tempo in tutta la sua integrità ed autenticità[5], sia come unità singola che in relazione ad altri documenti.

6. Il protocollo informatico

Le diverse unità organizzative che compongono la pubblica amministrazione ricevono e producono tutta una serie di documenti, la cui gestione richiede procedure complesse e regole ben definite. La gestione dei documenti costituisce il necessario supporto informativo per lo svolgimento delle attività amministrative[6].
L'evoluzione tecnologica ha portato ad un ripensamento delle modalità di attuazione delle suddette procedure, nell'ottica della loro ottimizzazione, grazie all'utilizzo degli strumenti informatici e telematici. Invero l'intera sequenza delle operazioni di gestione dei flussi documentali può essere automatizzata, migliorando l'efficienza dei processi attraverso l'eliminazione della frammentazione degli uffici di protocollo.
Il protocollo informatico, che può essere definito come l'insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzate dalle amministrazioni per la gestione dei documenti, rende possibile la realizzazione di una gestione completamente automatizzata dei flussi documentali, attesa la loro interconnessione funzionale.
All'interno della pubblica amministrazione, il protocollo informatico ha rappresentato, finora, il primo passo verso l'automazione dell'ufficio, mentre il supporto alla gestione di flussi documentali ne rappresenta il successivo. Analizzando, infatti, il problema nel suo complesso, si nota che, nei sistemi di *WorkFlow Management*, il protocollo informatico è, in realtà, solo uno dei momenti dell'automazione dei procedimenti amministrativi o, più in generale, del supporto all'informatizzazione dei processi o flussi di lavoro (*workflow*), che attiva una determinata procedura, automatizzata in tutte le sue fasi.
L'insieme di fasi che compongono l'*iter* automatizzato dei flussi documentali comprende la gestione di base, ossia il nucleo minimo, cui seguono la gestione documentale, l'informatizzazione documentale tramite *workflow*, il *Business Process Reengeneering*[7].

---

[5] E. MASSELLA DUCCI TERI, La conservazione alternativa dei documenti, in Interlex (www.interlex.it).

[6] G. Lombardi, *La normativa italiana per il protocollo*, in D. Piazza (a cura di), *Il protocollo informatico per la Pubblica amministrazione*, Maggioli, Rimini, 2003, p. 67.

[7] G. Butti, *Tecnologie e applicazioni per il protocollo informatico*, in D. Piazza (a cura di), cit., p. 147.

7. Il fascicolo informatico

La pubblica amministrazione titolare del procedimento può raccogliere in un fascicolo informatico gli atti, i documenti e i dati del procedimento medesimo da chiunque formati e, al momento della comunicazione dell'avvio del procedimento, informa gli interessati sulle modalità per esercitare in via telematica i diritti di cui all'articolo 10 della legge 7 agosto 1990, n. 241. In questo modo si vuole garantire che vengano accelerati i tempi e le procedure interne, con maggiore efficienza, minore costo per la PA e maggiore trasparenza per i cittadini.
Il d.lgs. 159/2006 ha novellato il comma 2 dell'art. 41 del codice del 2005, inserendovi tre commi. In particolare, il comma 2-bis, dispone che il fascicolo informatico è realizzato in modo tale da essere direttamente consultato e alimentato da tutte le amministrazioni coinvolte nel procedimento. Il comma 2-ter indica le informazioni che il fascicolo informatico deve contenere tra cui l'indicazione: dell'amministrazione titolare del procedimento, che cura la costituzione e la gestione del fascicolo medesimo; delle altre amministrazioni partecipanti; del responsabile del procedimento; dell'oggetto del procedimento; dell'elenco dei documenti contenuti, salvo quanto disposto dal successivo comma 2-quater, che, a sua volta, specifica che "il fascicolo informatico può contenere aree a cui hanno accesso solo l'amministrazione titolare e gli altri soggetti da essa individuati; esso è formato in modo da garantire la corretta collocazione, la facile reperibilità e la collegabilità, in relazione al contenuto ed alle finalità, dei singoli documenti; è inoltre costituito in modo da garantire l'esercizio in via telematica dei diritti previsti dalla citata legge n. 241 del 1990".
Il fascicolo informatico si pone come centro del procedimento telematico, quale punto di condivisione delle attività e delle informazioni su cui ogni ufficio o amministrazione può intervenire per conoscere o per immettere il proprio contributo per un determinato procedimento amministrativo[8].
Nella procedura automatizzata, tutta la documentazione informatica del procedimento risiede in un *server* del quale è responsabile l'amministrazione procedente.
Ogni attività amministrativa può, dunque, partire usufruendo dell'accesso ai fascicoli virtuali delle pratiche, perché l'accesso telematico non presenta limiti di sorta e può essere contemporaneo per tutti i partecipanti, trasformando, così, lo schema lineare e sequenziale del procedimento in uno schema a stella[9].

8. La conservazione digitale dei documenti amministrativi

Le pubbliche amministrazioni e i privati hanno la facoltà di sostituire i documenti dei propri archivi, le scritture contabili, la corrispondenza e degli altri atti di cui, per legge o regolamento, è prescritta la conservazione, con la loro riproduzione su supporto fotografico, su supporto

---

[8] G. Duni, *Codice dell'Amministrazione digitale: riflessioni de iure condendo*, in *Quaderni del DAE* (www.cesda.it), 2005.

[9] G. Duni, *Ancora sul procedimento amministrativo telematico: le ultime ricerche*, Relazione al DAE, III Convegno Nazionale sul Diritto Amministrativo elettronico, Catania, 2-3 luglio 2004, in *Quaderni del DAE* (www.cesda.it), 2005.

ottico o con altro mezzo idoneo a garantire la conformità dei documenti agli originali. Gli obblighi di conservazione e di esibizione dei documenti s'intendono soddisfatti, ai fini sia amministrativi sia probatori, anche se realizzati su supporto ottico.
Il problema della conservazione digitale dei documenti e del trasferimento degli archivi cartacei su supporti informatici attiene alla necessità di garantire l'efficacia legale sia dei documenti originali che degli archivi digitali. Sono gli strumenti della firma digitale e della marcatura temporale a garantire la corretta e affidabile conservazione del documento, qualunque sia la sua origine. Il processo di conservazione, infatti, si realizza attraverso la memorizzazione su supporto, di qualsiasi genere, dei documenti e, eventualmente, anche delle loro impronte, e termina con l'apposizione del riferimento temporale e della firma digitale sull'insieme dei documenti destinati alla conservazione o, se conveniente, su una evidenza informatica contenente una o più impronte dei documenti o di insiemi di essi.
Il codice dell'amministrazione digitale affronta la disciplina della conservazione dei documenti delle PA agli artt. 42 ss.
Nella specie, le pubbliche amministrazioni devono provvedere al recupero, su supporto informatico, dei documenti e degli atti cartacei dei quali sia obbligatoria od opportuna la conservazione e la riproduzione in digitale deve essere effettuata in modo tale da garantire la conformità dei documenti agli originali e la loro conservazione nel tempo.
Le amministrazioni devono, inoltre, predisporre degli appositi piani di sostituzione degli archivi cartacei con archivi informatici. Il sistema di conservazione permanente dei documenti con modalità digitali, cui può affiancarsi l'archiviazione con modalità cartacee per le esigenze correnti, garantisce l'identificazione certa del soggetto che ha formato il documento e dell'amministrazione di riferimento; l'integrità del documento; la leggibilità e l'agevole reperibilità dei documenti e delle informazioni indicative, inclusi i dati di registrazione e di classificazione originari; il rispetto delle misure di sicurezza in tema di trattamento dei dati personali.

9. Il diritto d'accesso telematico

Il codice dell'amministrazione digitale riconosce il diritto d'accesso telematico come diritto all'art. 52. L'accesso telematico è definito come la consultazione, per via telematica, degli archivi e dei documenti informatici delle pubbliche amministrazioni sia per la tutela di situazioni giuridicamente rilevanti da parte di chi ne abbia interesse, sia per le attività amministrative. E consiste, specificamente, nella visualizzazione e lettura del documento, e nell'estrazione, ossia nella stampa dello stesso o nella possibilità di copiarlo su altro supporto.
Quanto all'accesso telematico esterno, ogni amministrazione deve individuare le modalità di identificazione del richiedente, anche servendosi del sistema della firma digitale, e, a seguito dell'identificazione deve verificare la legittimazione ad accedere e l'assenza di cause limitative o esclusive dell'accesso. In tal modo, il richiedente ottiene i documenti e le informazioni, nei limiti di quanto stabilito da ciascuna amministrazione.
Diversamente, nel caso di accesso telematico interamministrativo, i dati sono resi accessibili e fruibili alle altre amministrazioni quando l'utilizzazione del dato sia necessaria per lo

svolgimento dei compiti istituzionali dell'amministrazione richiedente (art. 50, comma 2) e i rapporti tra amministrazione cedente e richiedente potranno essere disciplinati da apposite convenzioni, al fine di favorire la fruibilità informatica dei dati di cui sono titolari (art. 58, comma 2). Il trasferimento di un dato da un sistema informativo a un altro non modifica la titolarità del dato stesso (art. 58, comma 1) e l'accesso deve avvenire senza oneri, salvo solo il riconoscimento di eventuali costi eccezionali (art. 50, comma 2).
Le modalità di invio telematico delle richieste di accesso sono state disciplinate dal d.p.r. 12 aprile 2006, n. 184, regolamento recante disciplina in materia di accesso ai documenti amministrativi.

10. Il Sistema pubblico di connettività

La gestione dei procedimenti amministrativi informatici richiede per la sua attuazione che tutte le amministrazioni e gli enti siano dotati di un sistema informativo strutturato, non solo per favorire l'automazione delle funzioni e delle procedure interne dell'amministrazione e per l'erogazione dei servizi agli utenti, ma, anche, per consentire l'erogazione dei servizi direttamente ai sistemi informatici delle altre amministrazioni, per un migliore svolgimento delle rispettive funzioni.
Per questo, già nei primi progetti di coordinamento informatico per la PA è stato previsto che i sistemi informativi delle amministrazioni fossero connessi tramite una rete tra pari, che garantisse l'interconnessione telematica delle varie reti dell'amministrazione esistenti.
La prima rete ad essere istituita è stata la Rete Unitaria delle Pubbliche Amministrazioni (RUPA), volta a realizzare un sistema informativo unico di amministrazioni interagenti per la produzione di servizi a cittadini e imprese, con l'ottimizzazione delle risorse telematiche individuate in tre livelli applicativi: l'interconnessione, l'interoperabilità e l'area dei programmi applicativi.
I livelli applicativi della rete unitaria sono stati ridefiniti dal successivo d.lgs. 28 febbraio 2005, n. 42, che ha istituito il Sistema Pubblico di Connettività (SPC) e la Rete Internazionale della Pubblica Amministrazione (RIPA). Le norme in materia di SPC sono state inserite nel codice dell'amministrazione digitale, al capo VIII, dal d.lgs. 159/2006, che, peraltro, all'art. 84 ha stabilito che le amministrazioni che aderiscono alla RUPA, debbano presentare al CNIPA dei piani di migrazione verso il SPC.
Il SPC è "l'insieme di infrastrutture tecnologiche e di regole tecniche, per lo sviluppo, la condivisione, l'integrazione e la diffusione del patrimonio informativo e dei dati della pubblica amministrazione, necessarie per assicurare l'interoperabilità di base ed evoluta e la cooperazione applicativa dei sistemi informatici e dei flussi informativi, garantendo la sicurezza, la riservatezza delle informazioni, nonché la salvaguardia e l'autonomia del patrimonio informativo di ciascuna pubblica amministrazione" (art. 2, comma 2, d.lgs. 42/2005).
Le finalità che la realizzazione del SPC si propone sono, in particolare, quelle di fornire un insieme di servizi di connettività condivisi dalle pubbliche amministrazioni interconnesse; garantire l'interazione della pubblica amministrazione centrale e locale con tutti gli altri soggetti connessi a Internet, nonché con le reti di altri enti, promuovendo l'erogazione di servizi di qualità

e la miglior fruibilità degli stessi da parte dei cittadini e delle imprese; creare una infrastruttura condivisa di interscambio che consenta l'interoperabilità tra tutte le reti delle pubbliche amministrazioni esistenti; implementare lo sviluppo dei sistemi informatici nell'ambito del SPC. La Rete Internazionale delle Pubbliche Amministrazioni (RIPA), poi, costituisce l'infrastruttura di connettività che collega le pubbliche amministrazioni con gli uffici italiani all'estero, garantendo adeguati livelli di sicurezza e qualità (art. 3, comma 1, d.lgs. 42/2005; art. 74, comma 2, d.lgs. 159/2006).

11. Conclusioni

La legge 18 giugno 2009, n. 69, recante Disposizioni per lo sviluppo economico, la semplificazione, la competitività nonché in materia di processo civile, ha introdotto alcune disposizioni di modifica al codice dell'amministrazione digitale[10].
Il nuovo codice dell'amministrazione digitale ha riproposto la normativa del 2005 alla luce delle più recenti applicazioni informatiche e di nuovi obiettivi di efficacia e semplificazione della PA.
Punti salienti su cui concentra l'attenzione la riforma sono: la riorganizzazione delle pubbliche amministrazioni attraverso l'istituzione di un ufficio unico responsabile delle attività informatiche, la razionalizzazione organizzativa e informatica dei procedimenti, l'introduzione del protocollo informatico e del fascicolo elettronico; la semplificazione dei rapporti con i cittadini e con le imprese attraverso l'introduzione di forme di pagamenti informatici, lo scambio di dati tra imprese e PA, la diffusione e l'uso della posta elettronica certificata, l'accesso ai servizi in rete, l'utilizzo della firma digitale, la dematerializzazione del materiale documentale; l'organizzazione di piani di emergenza per garantire la continuità operativa nella fornitura di servizi e lo scambio di dati in caso di eventi disastrosi.
Gli obiettivi sono di ridurre i tempi e i costi per le pratiche amministrative, dando concreto avvio alla dematerializzazione del patrimonio informativo della PA e potenziando l'utilizzo della posta elettronica certificata. L'idea, infatti, è quella di far utilizzare alla PA soltanto la posta elettronica certificata per tutte le comunicazioni che richiedono una ricevuta di consegna a chi ha dichiarato il proprio indirizzo.

[10] Le principali informazioni relative alla recente riforma del codice dell'amministrazione digitale si possono consultare sui siti www.governo.it; www.saperi.forumpa.it; www.altalex.it; www.banchedati.camera.it.

Rivista elettronica di Diritto, Economia, Management

N. 1 - 2010 · pp. 137-161

La società dell'informazione tra egovernment e principio di sussidiarietà

Marco Mancarella

Abstract: In questi ultimi anni si è assistito alla nascita di un nuovo modello di società, la c.d. società dell'informazione, caratterizzata da una continua e rapida evoluzione delle tecnologie dell'informazione e della comunicazione. L'affermarsi di un nuovo modello di società, con i notevoli vantaggi che ne derivano, rappresenta, senza dubbio, un importante traguardo e, al contempo, il punto di partenza per quel cambiamento organizzativo e gestionale della pubblica amministrazione volto a migliorare i servizi per il cittadino e a rendere trasparente l'azione amministrativa, il tutto attraverso la piena realizzazione di un cd. governo elettronico, anche definito eGovernment. Conseguenza, dunque, di questa evoluzione è stato l'accentuarsi dell'attenzione dei Governi per le tecnologie dell'informazione e della comunicazione: esse sono uno strumento chiave per la trasformazione e l'integrazione delle amministrazioni degli Stati dell'Unione Europea, in quanto fattore abilitante del cambiamento. Le novità rappresentate dall'ingresso delle nuove tecnologie nel campo del diritto hanno però rivoluzionato numerosi istituti modificandone radicalmente la configurazione giuridica e costringendo il giurista a far proprie nozioni tecniche ed applicazioni informatiche. Tra questi istituti da rileggere in un'ottica digitale, sussiste di certo il principio di sussidiarietà, anch'esso di genesi comunitaria. Il presente contributo ne analizza la portata sia sotto il profilo della cd. sussidiarietà verticale digitale che sotto il restante profilo della cd. sussidiarietà orizzontale digitale, con il preciso fine di evidenziare in che modo i poteri e organi dello Stato oggi siano costretti a ripensare i loro rapporti e gerarchie in un contesto digitale e, quindi, di eGovernment.

The establishment of a new pattern of society, along with the benefits arising from it, it is with no doubts an important goal and, at the same time, the starting point for both an organizational and administrative change within the public administration aimed at improving citizen-oriented services as well as making the administrative action clear, through a full achievement of the so-called eGovernment, short for electronic government. However, innovations resulting from the advent of new technology applied to law have disrupted several institutions, changing radically their juridical configuration. So, the lawyer is compelled to gain technical knowledge and applications. The principle of subsidiarity, introduced into Community Law, certainly belongs to those institutions that need a digital new reading.

Articolo pervenuto il 12 ottobre 2010, approvato il 1 dicembre 2010

Parole chiave: società dell'informazione, eGovernment, sussidiarietà digitale.

Sommario: 1. L'eGovernment nell'odierna Società dell'Informazione - 2. Le politiche di eGovernment - 3. La sussidiarietà digitale verticale - 4. La sussidiarietà digitale orizzontale.

1. L'eGovernment nell'odierna Società dell'Informazione

Il dibattito sulle dinamiche connesse alla Società dell'Informazione risale agli anni Sessanta del secolo scorso e riconducibile all'idea di società post-industriale, sintetizzabile nella tendenza delle attività economiche ad indirizzarsi sul versante dei servizi. Sono gli anni in cui il crescente ruolo svolto dalla scienza e dalla tecnica nei processi produttivi, da un lato, e la conseguente introduzione delle tecnologie informatiche, dall'altro, determinano l'affermarsi di un nuovo *principio assiale* su cui si basano economia, politica e diritto. In tale contesto, informatica e tecnologia giocano un ruolo determinante sulla produzione del sapere, sulla gestione delle fonti informative, sulle nuove modalità di conduzione degli scambi economici, sull'amministrazione pubblica, sui nuovi diritti.
L'informazione è trattata come una merce ed è immessa nel mercato ad un prezzo determinato o determinabile: conseguentemente, il possesso d'informazioni rappresenta la più importante fonte di potere, mentre le tecnologie informatiche si affermano quali forti strumenti di direzione e controllo[1]. Un ulteriore contributo, sempre negli stessi anni, propone il superamento del concetto di classe tipico del processo di industrializzazione capitalistica, al quale si lega il conflitto tra tecnocrati da una parte ed una configurazione sociale più eterogenea dall'altra, i cui mezzi di sussistenza e stili di vita sono controllati dai primi[2]. Anche secondo questa linea di pensiero, la posta in gioco non è il patrimonio materiale, ma il possesso della conoscenza, dell'informazione e il controllo delle stesse.
Alla fine degli anni Ottanta si afferma, con la Scuola inglese, un nuovo "*paradigma tecnologico*" basato sull'idea che le tecnologie agiscono sull'informazione e quest'ultima sulle tecnologie, determinando nuovi livelli d'interconnessione[3]; l'informazione, però, è concepita come parte integrante dell'intera attività umana, quindi il suo legame con il sistema tecnologico determina effetti su tutti i processi dell'esistenza umana.
Gli anni Novanta rappresentano per i Paesi UE il momento di maggiore e più diffusa attenzione sul tema. L'imponente sviluppo delle tecnologie ICT è coniugato all'esigenza di migliorare in modo sostanziale qualità e quantità dell'informazione e dei servizi ad essa connessi. Espressione di questo sforzo congiunto è la redazione del *Rapporto Delors* (1993), con il quale si formalizza la definizione di "*Società dell'Informazione*", e la successiva redazione del Rapporto "*eEurope. Una Società dell'Informazione per tutti*" (1994), che consolida i contenuti del lavoro precedente e delinea l'impegno istituzionale dell'Unione Europea a valorizzare

---

1 Cfr. Bell D., *The coming of post-industrial society*, New York, Basic Books, 1973.

2 Cfr. Touraine A., *La società post-industriale*, Bologna, Il Mulino, 1970.

3 Cfr. Castells M., *End of millenium*, Oxford, Maldel, 2000.

l'informazione e gestirla come bene comune della società. Nella Società dell'Informazione l'utilizzo delle ICT determina una sorta di rivoluzione per molti aspetti simile a quella industriale, ma con un potenziale di diffusione privo di limiti temporali o confini geografici, dettato dall'interscambio di dati, rapido ed efficace, tra soggetti di diritto (privati, cittadini, imprese, organizzazioni istituzionali e amministrazioni pubbliche), un sistema, quindi, in grado di disegnare nuovi modelli sociali, politici ed economici al centro dei quali vi è lo scambio di conoscenza[4]. La ricostruzione temporale-evolutiva del tema, le politiche internazionali e gli impegni istituzionali assunti a livello europeo, oltre che nazionale, rappresentano la premessa per valutare aspettative sociali, economiche, giuridiche nell'ambito della complessa relazione tra gestione informativa e sviluppo sostenibile[5].

Ma è nel 1996 con il Libro verde "*Living and working in the information society: people first*". che si sottolinea la centralità della dimensione umana. Obiettivo: "*Una società per tutti*". Tra le successive iniziative europee in materia si ricorda il *"Programma pluriennale per la realizzazione della Società dell'Informazione"*, adottato con Decisione del 30 Marzo 1998, con il quale il Consiglio dell' UE sottolinea l'importanza dell'instaurarsi di nuove forme di relazione economica, politica e sociale favorite dalla Società dell'Informazione.

Una delle sfide prioritarie per la Commissione Europea, per rendere le pubbliche amministrazioni più efficaci e più vicine al cittadino, è rappresentata dall'uso delle tecnologie dell'informazione e della comunicazione. A tal fine l'Unione Europea si rivolge alle amministrazioni pubbliche (a livello nazionale e locale) per sostenerle nel processo di trasformazione e riforma dando vita alle politiche di "governo elettronico", anche detto "eGovernment", ed ai conseguenti piani di azione, con la finalità di garantire il confronto tra esperienze diverse per favorire la diffusione di *best practices* e soluzioni innovative per un più efficiente utilizzo delle risorse e un più facile raggiungimento degli obiettivi di Lisbona.

In quest'ottica d'implementazione della Società dell'Informazione attraverso il processo d'innovazione della Pubblica Amministrazione europea si colloca la problematica del presente contributo. Nello specifico, di seguito s'intende affrontare la questione connessa al rapporto tra più livelli di potere pubblico ai fini di un'effettiva realizzazione dell'eGovernment nell'odierna Società dell'Informazione, rapporto caratterizzato dal necessario rispetto del principio comunitario di sussidiarietà, inteso sia in senso verticale che orizzontale. L'analisi, non potendo scendere nelle particolari esperienze dei singoli stati membri, disamina questa che comporterebbe la necessità di un lavoro monografico, si concentrerà sull'esperienza italiana e, dunque, sullo stretto connubio esistente oggi nel nostro ordinamento tra strumenti della Società dell'Informazione, politiche di eGovernment e principio di sussidiarietà.

---

[4] Cfr. Preite G., *Il riconoscimento biometrico. Sicurezza versus privacy*, Trento, UNI Service, 2008.

[5] In questa specifica sede verrà affrontata la questione della sostenibilità valutando l'impatto delle tecnologie informatiche e dell'informazione sulle attività turistiche, nelle sue specifiche forme. La definizione base di "sviluppo sostenibile" che si considererà è quella formulata nel 1987 dal Rapporto Brundtland nell'ambito della Commissione O.N.U. su Ambiente e Sviluppo, secondo cui si deve intendere per "sviluppo sostenibile" quella particolare forma di sviluppo in grado di soddisfare "i bisogni dell'attuale generazione senza compromettere la capacità di quelle future di rispondere ai loro".

2. Le politiche di eGovernment

Il primo passo da compiere in uno studio incentrato sul concetto di *eGovernment* è quello volto alla comprensione e all'approfondimento etimologico del medesimo termine.
Il termine *eGovernment* deriva dall'acronimo inglese "e" = *electronic* e "*government*" = governo: letteralmente, dunque, "governo elettronico". Ma limitarsi ad una definizione del termine così superficiale e letterale, considerata la ricchezza delle sue sfaccettature ed applicazioni, non è possibile.
Per *eGovernment*, pertanto, è giusto intendere, secondo una recente esplicitazione in grado di cogliere il meglio delle varie definizioni che negli ultimi anni sono state proposte a livello politico e normativo, "l'ottimizzazione continua nell'erogazione dei servizi, nella partecipazione dei cittadini, nella *governance*, attraverso la trasformazione delle relazioni interne ed esterne per mezzo delle tecnologie, di Internet e dei nuovi mezzi di comunicazione di massa, combinati con i cambiamenti organizzativi e le nuove professionalità richieste per migliorare i servizi pubblici e i processi democratici, il tutto finalizzato a supportare le politiche pubbliche"[6].
Una definizione complessa, come quella ora richiamata, sembra condurre l'interprete verso un nuovo approccio al tema. L'*eGovernment* diviene il grimaldello per scardinare l'arcaico concetto di Amministrazione, a favore di una nuova visione della Cosa Pubblica incentrata sull'innovazione, ovvero su di un mutamento complesso nel contesto ambientale, nell'organizzazione, nella tecnologia, in grado di condurre ad una miscela di eventi e risorse che conduca al cambiamento: detto in altre parole, l'*eGovernment* come *iGovernment*, ove la "i" rappresenta la necessaria innovazione procedurale e organizzativa di cui la Pubblica Amministrazione ha bisogno per il raggiungimento dei paramenti di efficacia, efficienza economicità prescritti nel nostro ordinamento[7].
L'*eGovernment* si palesa, dunque, come la massima espressione dell'applicazione dell'*Information and Communication Technology* (ICT) all'apparato pubblico, o anche l'espressione "pubblica" delle ICT nell'odierna "Società dell'Informazione".
All'interno dei modelli di *eGovernment* occorre distinguere quattro categorie o spazi di sviluppo per l'Amministrazione elettronica: il modello G2C (*Government to Citizen*) riguarda lo sviluppo di servizi con destinatario il singolo individuo in quanto cittadino; il modello G2B (*Government to Business*) riguarda invece lo sviluppo dei servizi governativi con destinatari le imprese e gli attori economici; il modello G2E (*Government to Employee*) riguardante lo sviluppo dei servizi in seno alla stessa Amministrazione con destinatari gli impiegati ed i funzionari; il modello G2G (*Government to Government*) riguardante, infine, lo sviluppo di servizi e applicazioni volti ad instaurare o migliorare la collaborazione e la cooperazione tra i servizi delle diverse istituzioni governative[8].

---

6 A. Romano, L. Marasso, M. Marinazzo, *Italia chiama eGovernment*, Milano, Guerini e Associati, 2008, p. 26. Nel testo citato è possibile approfondire le varie definizioni di *eGovernment* affermatesi negli ultimi anni su scala nazionale e internazionale.

7 *Ibidem*.

8 S. Assar, I. Boughzala (a cura di), *Administration électronique: constats et perspectives*, Paris, GET et Lavoisier, 2007, p. 21;

Oggi l'*eGovernment* si fonda principalmente su quattro obiettivi principali: 1) raccolta del maggior numero di informazioni in uno spazio sempre più ridotto; 2) trattamento e trasmissione delle informazioni ad una velocità sempre maggiore; 3) interscambio delle informazioni (interoperabilità), anche se raccolte con tecniche e linguaggi diversi; 4) conservazione (non deperibilità) e sicurezza (non modificabilità da parte di soggetti non autorizzati) delle informazioni[9].

L'*eGovernment*, inteso come complesso delle politiche di introduzione delle ICT nelle Pubbliche Amministrazioni, non ha avuto sempre gli stessi obiettivi e soltanto negli ultimi anni si è iniziato a considerarlo in termini unitari, con una forte attenzione ai contenuti e all'impatto organizzativo nei processi di informatizzazione delle attività e dei processi. In questo senso si può parlare, laddove essa si realizza, di una organica politica di *eGovernment,* in cui non è più sufficiente creare infrastrutture e reti di interconnessione, né è sufficiente ampliare l'accesso alle informazioni con la creazione di servizi informativi aperti se, poi, non si è in grado di garantire che tutte le informazioni detenute dalle Amministrazioni siano raccolte e conservate in formato elettronico e messe a disposizione avvalendosi delle ICT, e se le Amministrazioni non siano in grado di assicurare la necessaria qualità delle informazioni raccolte e la loro necessaria sicurezza[10].

Il passaggio dalla semplice creazione di infrastrutture e reti di interconnessione ad una gestione "sicura" di dati digitali qualitativamente certi è facile ravvisarlo analizzando semplicemente i documenti programmatici del nostro Governo italiano in tema di *eGovernment* nell'ultimo ventennio.

In Italia è possibile suddividere il periodo di attuazione dell'*eGovernment* in tre fasi: una prima fase dal 2001 al 2003, una seconda fino al 2005 ed una terza ad oggi ancora in corso, avviatasi con l'approvazione nel 2005 del Codice dell'Amministrazione Digitale[11].

---

[9] In argomento si veda: Merloni F. (a cura di), *Introduzione all'eGovernment*, Torino, Giappichelli, 2005; W. D'Avanzo, *L'e-government*, MoviMedia, Lecce, 2007.

[10] Merloni F. (a cura di), *Introduzione all'eGovernment*, op. cit., pp. 9-12.

[11] Volendo fare un discorso più ampio rispetto a quello della semplice "attuazione" dell'eGovernment e, dunque, volendo analizzare le fasi storiche di evoluzione dell'informatica nella Pubblica Amministrazione, esse possono essere così sintetizzate: a) la prima fase è consistita nell'informatizzazione parziale, da parte di singole Amministrazioni Pubbliche, di attività amministrative, con il prevalente obiettivo di semplificarne l'esercizio e ridurne il costo, sostituendo il lavoro umano con le capacità di elaborazione automatica (anni '50-'60 del secolo scorso); b) in una seconda fase, resa possibile dall'accresciuta capacità di calcolo e di elaborazione dell'ICT, le singole Amministrazioni si sono poste obiettivi più generali, consistenti nella integrale informatizzazione di tutte le proprie attività (anni '70-'80 del secolo scorso); c) una terza fase si è aperta allorché è stato posto il problema della interconnessione tra i sistemi informativi delle diverse Amministrazioni Pubbliche per consentire tra esse uno scambio di informazioni in grado di semplificare lo svolgimento delle attività amministrative, con l'obiettivo, quindi, della creazione di una rete unitaria delle Pubbliche Amministrazioni (anni '90 del secolo scorso); d) nella quarta fase, le nuove ICT hanno permesso di utilizzare tutte le potenzialità offerte dalla rete con un approccio del tutto nuovo al problema dei rapporti con l'esterno, ponendo al centro cittadini e imprese (primo decennio del XXI secolo). Per una visuale completa dell'evoluzione politico-normativa dell'informatica pubblica e, conseguentemente, dell'*eGovernment*, si veda: P. Giacalone, *La normativa sul governo elettronico*, Milano, Franco Angeli, 2007; C. Rabbito, *L'informatica al servizio della Pubblica Amministrazione e del cittadino*, Bologna, Gedit Edizioni, 2007; A. Contaldo, *Dalla teleamministrazione all'e-government: una complessa transizione in fieri*, in "Foro Amministrativo", n. 4, 2002, pp. 1111-1127; G. Duni, *Teleamministrazione* (voce), in *Enciclopedia Giuridica Treccani*, Roma, XXX, n. 5, 1993.

La prima fase di attuazione dell'*eGovernment*, nelle Regioni e negli Enti Locali, si è sviluppata, come detto, a cavallo tra 2001 ed il 2003, lungo tre linee di azione tra loro interconnesse:

1. promozione di progetti di *eGovernment* nelle Regioni e negli Enti Locali, volti allo sviluppo di servizi infrastrutturali e di servizi finali per cittadini e imprese;
2. definizione di un comune quadro di riferimento tecnico, organizzativo e metodologico per la realizzazione di progetti di *eGovernment*;
3. creazione, su tutto i territorio nazionale, di Centri Regionali di Competenza (CRC), aventi come obiettivo il sostegno alle Regioni e agli Enti Locali per la preparazione e realizzazione di progetti di *eGovernment*[12].

In tale prima fase, il Ministro per l'innovazione e le tecnologie ha stabilito, con Decreto del 14 novembre 2002, un finanziamento di 120 milioni di euro, di cui 80 per 98 progetti in grado di realizzare servizi ai cittadini e alle imprese[13].

Ulteriore passo in avanti lungo la strada dell'*eGovernment* è stato compiuto nel 2001, con la creazione del Ministero per l'Innovazione e le Tecnologie, presieduto dal Ministro Stanca, volto a soddisfare l'esigenza di un coordinamento centrale sulle iniziative di sviluppo e diffusione delle nuove tecnologie, il tutto attraverso l'esercizio di molte delle deleghe in tema di innovazione, precedentemente appartenute alla Funzione Pubblica e ad altri ministeri.

Il 2001 è da considerarsi un anno fondamentale dal punto di vista dell'innovazione normativa, con riforme che cambiano i tradizionali rapporti tra centro e periferia. Prende avvio e si consolida la Riforma del Titolo V della Costituzione, approvato con la Legge Costituzionale n. 3/2001, dal titolo "Modifiche al titolo V della parte seconda della Costituzione". La Riforma del 2001 è incentrata sul decentramento amministrativo, attraverso la delega, di gran parte delle funzioni amministrative del Governo a Regioni ed Enti locali. Ciò ha comportato, nell'ottica di una riorganizzazione dei poteri pubblici dal basso verso l'alto, l'affermazione del principio di sussidiarietà, favorendo i livelli di Amministrazione più vicini al cittadino, con l'obiettivo di rivalutare il rapporto tra cittadinanza e Pubblica Amministrazione, incanalando gli interventi dello Stato in un'azione maggiormente efficace in quanto ramificata sul territorio. La Riforma del 2001 si fonda, in definitiva, sul medesimo principio cardine sotteso al "pacchetto Bassanini" del 1997[14], con il quale si è intrapresa, concretamente, la strada del decentramento amministrativo.

Nel 2002 sono state pubblicate dal Ministro Stanca le "Linee Guida del Governo per lo sviluppo della Società dell'Informazione", contenenti 10 obiettivi prioritari, da raggiungere entro la legislatura, raggruppati in 5 macro aree (servizi on-line ai cittadini e imprese, efficienza, valorizzazione delle risorse umane, trasparenza, qualità), volti a fornire indicazioni rispetto

---

[12] L. Marasso, *Manuale dell'eGovernment*, Santarcangelo di Romagna, Maggioli, 2005, pp. 144-156.

[13] Le risultanze di dei progetti di *eGovernment* predisposti in Italia nei primi anni del uovo millennio sono state attentamente analizzate nel testo: Presidenza Consiglio dei Ministri-Dipartimento della Funzione Pubblica, *eGovernment e organizzazione nelle Amministrazioni Pubbliche. Analisi di caso sulle leve e le condizioni organizzative per l'efficacia dell'eGovernment*, Soveria Mannelli, Rubbettino, 2007.

[14] Per "pacchetto Bassanini" si intende: la L. n. 59/97, la L. n. 127/97 e il D.Lgs. n. 112/98. Per un approfondimento del contenuto del "pacchetto Bassanini" e della sua importanza nel quadro delle politiche di *eGovernment* si veda: A. Romano, L. Marasso, M. Marinazzo, *Italia chiama eGovernment*, op. cit., pp. 61-68.

allo sviluppo dei progetti di *eGovernment* nel nostro Paese. La Pubblica Amministrazione inizia ad essere intesa come fornitrice di servizi.
In tale prima fase è stato importante è il ruolo assunto dalle Regioni nell'implementazione di processi di *eGovernment* sul territorio e nella predisposizione di servizi infrastrutturali per gli enti locali, i cittadini e le imprese, con un forte coinvolgimento degli enti più vicini al cittadino, i Comuni, nella direzione di una più ampia cooperazione tra Amministrazioni, sia di natura orizzontale che verticale.
Nell'ottica di un sempre maggiore coordinamento tra centro e periferia, prende vita nella primavera del 2002 il FORMEZ – Centro di Formazione Studi e, con l'art. 176 del Dlgs n.196/2003, il Centro Nazionale per l'Informatica nella Pubblica Amministrazione (CNIPA). Il CNIPA sostituisce l'Autorità per l'Informatica nella Pubblica Amministrazione (AIPA), creata con il D.Lgs. n. 39/93, e si occupa della progettazione e dell'implementazione dell'*eGovernment*. Il confronto tra CNIPA, Regioni ed Enti Locali ha poi permesso di definire gli obiettivi e le modalità di realizzazione della seconda fase dell'*eGovernment*.
La seconda fase di attuazione è stata avviata su approvazione della Conferenza Unificata Stato, Regioni, Città e Autonomie locali il 27 novembre 2003 e si è posta come obiettivo principale l'allargamento alla maggior parte delle Amministrazioni locali dei processi di innovazione già avviati, attraverso il "riuso" delle iniziative realizzate nella prima fase, sia per ciò che concerne l'organizzazione di servizi per cittadini e imprese che la realizzazione di servizi infrastrutturali in tutti i territori regionali.
L'introduzione delle nuove tecnologie dell'informazione e della comunicazione, a seguito dell'avvio di questa seconda fase di *eGovernment*, ha iniziato ad interessare concretamente l'attività di tutti i livelli istituzionali. Infatti, la concertazione tra Governo, Regioni e Autonomie locali ha condotto, nel 2005, all'emanazione del Codice dell'Amministrazione Digitale (CAD) con D.lgs. n. 82/2005, con il preciso obiettivo di realizzare una Pubblica Amministrazione efficiente e amica, erogante servizi ICT caratterizzati da immediatezza e trasparenza[15]. Inizia con il CAD la terza fase di attuazione dell'*eGovernment* nel nostro Paese.
Il Codice, da un lato, ha riconosciuto ai cittadini il diritto di interagire sempre e dovunque verso qualsiasi Amministrazione attraverso Internet, la Rete, la posta elettronica (Art. 3 CAD)[16] e, dall'altro, ha stabilito che tutte le Amministrazioni devono riorganizzarsi in modo da rendere sempre e comunque disponibili tutte le informazioni in modalità digitale (art. 2, comma 1, CAD)[17]. Il Codice, in definitiva, si propone come una summa normativa del mondo digitale

---

[15] Per un commento al Codice si rinvia a: E. Belisario, *La nuova Pubblica Amministrazione Digitale*, Santarcangelo di Romagna, Maggioli Editore, 2009; M. Quaranta (a cura di), *Il Codice della Pubblica Amministrazione Digitale*, Napoli, Liguori Editore, 2006; A. Cacciari, R. Cauteruccio, *Codice dell'Amministrazione Digitale: commentario*, Roma, Istituto Poligrafico e Zecca dello Stato, 2008.

[16] Art. 3 CAD: "I cittadini e le imprese hanno diritto a richiedere ed ottenere l'uso delle tecnologie telematiche nelle comunicazioni con le Pubbliche Amministrazioni e con i gestori di pubblici servizi statali nei limiti di quanto previsto nel presente codice.
1-bis. Il principio di cui al comma 1 si applica alle Amministrazioni regionali e locali nei limiti delle risorse tecnologiche ed organizzative disponibili e nel rispetto della loro autonomia normativa.
1-ter. Le controversie concernenti l'esercizio del diritto di cui al comma 1 sono devolute alla giurisdizione esclusiva del giudice amministrativo".

[17] Art. 1, comma 2, CAD: "Lo Stato, le regioni e le autonomie locali assicurano la disponibilità, la

che tiene conto di diritti e doveri e allo stesso tempo fornisce gli strumenti operativi con cui poterli concretizzare.

Il Codice disciplina una serie di materie di fondamentale importanza per una concreta digitalizzazione dell'apparato amministrativo e della relazione con il cliente/cittadino. Tra tali materie si ricorda: la disciplina della Posta Elettronica Certificata, avente, quest'ultima, lo stesso valore di una raccomandata con ricevuta di ritorno (artt. 6 e 48-49 CAD); la disciplina della firma digitale, volta a garantire con sicurezza l'identificazione e la volontà di firmare (artt. 24-37 CAD); la disciplina in tema di documento informatico che, sottoscritto con la firma digitale, detiene la medesima validità del documento cartaceo (artt. 20-23 CAD); la disciplina in tema di siti Internet della Pubblica Amministrazione, vincolante per quanto attiene alle caratteristiche di accessibilità, usabilità, semplicità e comprensibilità di linguaggio, affidabilità della navigazione e omogeneità (artt. 40-47 CAD); le Carte Elettroniche, ossia la Carta d'Identità elettronica e la Carta Nazionale dei Servizi, diventano, infine, strumenti chiave per razionalizzare e semplificare l'azione amministrativa (art. 66 CAD). Funzione essenziale degli strumenti ora richiamati è quella di avvicinare i cittadini alle attività delle istituzioni, al fine di realizzare una piena "democrazia digitale", anche detta *eDemocracy* ed un sistema di *eService delivery*. Più nello specifico, per *eDemocracy* dobbiamo intendere "tutte le attività attraverso le quali il Governo raccoglie le opinioni dei cittadini e delle imprese su un ampio numero di materie, dal cambiamento di leggi e regolamenti alla modifica di aspetti gestionali di specifici programmi e servizi"[18]; per *eService delivery* occorre considerare, invece, "la fornitura di servizi pubblici a cittadini e imprese attraverso i *network* digitali e i media, indipendentemente dal fatto che l'erogazione sia materialmente effettuata da un ente pubblico oppure da un soggetto privato sulla base di contratti o licenze"[19].

Il profilo dell'*eDemocracy* e dell'*eService delivery* ha anche dettato il contenuto dell'art. 9 del CAD, intitolato emblematicamente "Partecipazione democratica elettronica", in base al quale "Lo Stato favorisce ogni forma di uso delle nuove tecnologie per promuovere una maggiore partecipazione dei cittadini, anche residenti all'estero, al processo democratico e per facilitare l'esercizio dei diritti politici e civili sia individuali che collettivi". La norma ha un chiaro contenuto programmatico e non immediatamente precettivo, per alcuni "avveniristico"[20], ma di certo utile nel dettare negli anni al legislatore e all'Amministrazione Pubblica la via da seguire.

---

gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione in modalità digitale e si organizzano ed agiscono a tale fine utilizzando con le modalità più appropriate le tecnologie dell'informazione e della comunicazione".

[18] L. Buccoliero, *Il governo elettronico*, Milano, Tecniche Nuove, 2009, p. 7. Taluni Autori per rappresentare il concetto di *eDemocracy* utilizzano altri termini, ovvero: *Digital Democracy* (J. Caldow, *The quest for electronic government: a defining vision*, Washington DC, Institute for Electronic Government, 1999) o *Cyberdemocracy* (D. Holmes, *Egov: E-Business strategies for government*, London, Nicholas Brealey Publishing, 2001).

[19] *Ibidem*. L'*eDemocracy* e l'*eService delivery* vengono spesso inquadrate come due delle quattro fondamentali aree del governo elettronico, insieme all'*eManagement* (l'utilizzo dei mezzi digitali per allocare/riallocare risorse, finanziarie e personali, tra attività che fanno parte di strategie già definite) e l'*eGovernance* (l'applicazione delle nuove tecnologie alla formulazione delle *policy* e alla verifica e controllo del raggiungimento dei risultati).

[20] Cfr. A. Cacciari, *Commento art. 9 CAD* in M. Atelli, S. Aterno, A. Cacciari, R. Cauteruccio, *Codice dell'Amministrazione Digitale: commentario*, op. cit., pp. 27-28.

Se in Italia sono stati compiuti questi notevoli passi, in ambito continentale la Commissione Europea nel medesimo periodo, giugno del 2005, ha realizzato modifiche ed integrazioni alle iniziative comunitarie sull'*eGovernment*, approvando il documento "i2010 *eGovernment Action Plan*". Tale documento rappresenta il nuovo quadro strategico della Commissione europea che definisce gli orientamenti di massima per la Società dell'Informazione ed i media. Questa nuova politica integrata mira, in particolare, ad incoraggiare la conoscenza e l'innovazione per sostenere la crescita, nonché la creazione di posti di lavoro più numerosi e di migliore qualità[21].
Per fare fronte alle nuove esigenze dettate in via programmatica in ambito europeo, in Italia si è ritenuto opportuno, nel medesimo periodo, procedere ad un accorpamento, sotto un'unica regia politica, della funzione pubblica e dell'innovazione tecnologica, quale opportunità per incidere maggiormente sui meccanismi in grado di rendere più efficace l'*agere* amministrativo: tale scelta ha portato alla nascita del Ministero per la Pubblica Amministrazione e l'innovazione[22].
All'inizio del 2007 il Ministro per le Riforme e le Innovazioni nella Pubblica Amministrazione Luigi Nicolais ha presentato le "Linee strategiche sull'*eGovernment*", seguite dalla "Direttiva Innovazione". Questi documenti hanno rafforzato il concetto centrale della "Strategia di Lisbona"[23]: la costruzione di una società basata sulla conoscenza, nella quale il settore pubblico non deve rinunciare al proprio ruolo abilitante, per rendere il Paese più competitivo. La centralità del cittadino diviene l'idea chiave intorno alla quale deve ruotare la politica di *eGovernment* nazionale, quindi maggiore attenzione alla revisione dei processi di lavoro interni alla Pubblica Amministrazione finalizzata ad una maggiore partecipazione dei singoli e ad un decentramento del potere.
Si è giunti, infine, al Piano di *eGovernment* 2012, predisposto dalla Presidenza del Consiglio dei Ministri nel dicembre 2008, e volto a tracciare le linee d'intervento nei vari settori della Pubblica Amministrazione. L'obiettivo esplicito è quello di una definitiva affermazione dell'*eGovernment* nel nostro Paese che, sebbene fosse partito anche in anticipo rispetto al resto dell'Europa, si trova oggi in ritardo nel settore[24]. Per colmare il divario, il Governo italiano pare cogliere l'esigenza di discontinuità rispetto alle politiche del passato, fondate si sull'innovazione tecnologica ma non sulla lotta ai privilegi e alle sacche di inefficienza. Sembra profilarsi una Pubblica Amministrazione che, mutuando il pensiero di Joseph Schumpeter,

---

[21] Per un'analisi più approfondita del documento "i2010 *eGovernment Action Plan*" della Commissione Europea si rinvia all'URL, visionato nel mese di ottobre 2009: http://europa.eu/legislation_summaries/employment_and_social_policy/job_creation_measures/c11328_it.htm.

[22] Si rimanda all'URL: http://www.funzionepubblica.it/.

[23] In occasione del Consiglio Europeo tenutosi nel marzo del 2000, i capi di Stato e di Governo hanno ritenuto necessario avviare una nuova strategia, detta appunto "Strategia di Lisbona", volta a rendere l'economia europea la più competitiva su scala globale, con il contestuale risultato, abbastanza utopico, di una piena occupazione entro il 2010. La Strategia si fonda su tre pilastri: il primo, di natura economica, incentrato sulla necessità di adattarsi continuamente alle evoluzioni della società dell'informazione e sulle iniziative da incoraggiare in materia di ricerca e di sviluppo; il secondo, di natura sociale, incentrato sulla necessità di favorire investimenti nell'istruzione e nella formazione e su di una politica attiva per l'occupazione, onde agevolare il passaggio all'economia della conoscenza; il terzo, di ordine ambientale, strutturato sulla consapevolezza che la crescita economica vada dissociata dall'utilizzazione delle risorse naturali.

[24] Per la visione del Piano di eGovernment 2012 si rimanda all'URL, visionato nel mese di ottobre 2009: http://www.funzionepubblica.it/ministro/in_evidenza/6662.htm.

incentrato sull'impresa, e trasferendolo nella sfera pubblica[25], inizia ad "intraprendere" "nei servizi al Cittadino ed alle imprese, introduce nuovi servizi, sfrutta le innovazioni tecnologiche, apre a nuove fasce di utenti per i servizi rinnovati, cambia le modalità organizzative della produzione dei servizi"[26].

Nella direzione della politica unitaria di *eGovernment* (o di un coordinamento unitario di distinte politiche pubbliche) restano da segnalare alcuni nodi problematici ancora non risolti, soprattutto quanto alla loro compiuta individuazione e disciplina giuridica.

Il primo è costituito dalle difficoltà che si frappongono alla completa "digitalizzazione" delle informazioni raccolte in documenti formati su supporto cartaceo. Si tratta di difficoltà in gran parte legate ad una "percezione falsata" della sicurezza, di conseguenza, pur ponendosi l'obiettivo della piena digitalizzazione, si preferisce, prudenzialmente, doppiare la formazione del documento informatico con una copia su supporto cartaceo.

Il secondo nodo consiste nel necessario (ma non ancora realizzato) passaggio da una semplice sostituzione del supporto tecnologico dei documenti presso le singole Amministrazioni ad una integrata politica di inclusione/trattamento dell'intero patrimonio informativo di pubblico interesse. Da qui, il tema generale della valorizzazione del patrimonio informativo pubblico rivela due profili rilevanti: uno, culturale, che attiene al contributo che esso può dare alla crescita civile e democratica della collettività; ed uno economico, che attiene alla possibilità di attribuire, con elaborazioni informatiche, valore aggiunto alle informazioni e di sfruttarlo commercialmente[27].

Il terzo nodo è costituito dalla necessità di garantire adeguatamente i diritti connessi allo sviluppo delle ICT. Le nuove tecnologie, infatti, consentono una maggiore tutela dei diritti consolidati e tradizionali (l'accesso ai documenti per la tutela delle situazioni giuridiche, la disponibilità di informazioni per l'esercizio del controllo democratico sull'attività delle Amministrazioni)[28], ma fanno anche emergere diritti "nuovi". Si pensi, ad esempio, al cd. diritto all'uso delle tecnologie da parte della Pubblica Amministrazione, azionabile giudizialmente da qualsiasi cittadino/impresa in base al già menzionato art. 3 CAD[29].

Per comprendere appieno il tema dei "nuovi diritti" e la possibile relazione con le nuove tecnologie, è giusto approfondire il pensiero di Norberto Bobbio.

Per Bobbio tutte le generazioni di diritti si radicano fondamentalmente nella storia e non nella natura, non sono perciò espressione di principî assoluti ma di rivendicazioni umane affermatisi nel tempo. Infatti, "i diritti dell'uomo, pur fondamentali che siano, sono diritti storici, vale a dire, nati in certe circostanze, contrassegnate da lotte per la difesa di nuove libertà contro vecchi poteri, gradualmente, non tutti in una volta e non una volta per sempre". In base a

---

[25] Cfr. J. Schumpeter, *L'essenza e i principî dell'economia teorica*, Roma-Bari, Laterza, 1982; Id. *Il ciclo economico*, Salerno, Palladio, 1979.

[26] A. Romano, L. Marasso, M. Marinazzo, *Italia chiama eGovernment*, op. cit., p. 37.

[27] Questo secondo profilo è oggetto di una specifica politica comunitaria di coordinamento delle politiche degli stati membri, ancora molto "leggera". Si veda in particolare la Direttiva 2003/98/CE e la Direttiva 2007/2/CE che istituisce una "Infrastruttura per l'informazione territoriale nella Comunità europea (INSPIRE)".

[28] F. Merloni, (a cura di), *Introduzione all'eGovernment*, op. cit., p. 13.

[29] Si rimanda al contenuto della nota n. 12.

tale visione storicistica del diritto, l'Autore individua quattro precise generazioni di diritti: i diritti fondamentali (diritti di libertà), sociali (diritto al lavoro, all'istruzione, all'assistenza e altri), ecologici (diritto a vivere in un ambiente non inquinato) e genetici (diritto a non vedere manipolato il proprio patrimonio genetico)[30]. I "nuovi diritti" più fortemente connessi allo strumento ICT sono difficilmente collocabili nelle categorie bobbiane, (si pensi al diritto all'uso delle tecnologie da parte della PA, azionabile giudizialmente da qualsiasi cittadino/impresa). Tale difficile collocazione, rende lecita la supposizione dell'esistenza, oggi, di una quinta generazione di diritti: i diritti informatici.

Ma tale espressione, nella sua portata di certo rivoluzionaria, comporta, come ogni cambiamento radicale di agire: 1) un nuovo configurarsi dello stesso ruolo del cittadino e dei suoi diritti; 2) accompagnato da una trasformazione dell'autorità pubblica, sempre più diretta verso una naturale deconcentrazione del potere.

Sotto il primo profilo, quello attinente al nuovo ruolo del cittadino, prende sempre più forma il concetto di "cittadino elettronico", ovvero un cittadino non solo in grado di partecipare più attivamente alla vita democratica attraverso l'ausilio delle ICT (si pensi ad esempio alla possibilità di *forum* pubblici sul *web* per l'elaborazione di una proposta di legge popolare) ma anche in grado di usufruire di servizi innovativi da parte della Pubblica Amministrazione (si pensi al pagamento delle imposte *online*)[31].

Prende forma la già citata *eDemocracy*, ovvero una nuova forma di sistema democratico incentrato sull'ausilio delle nuove tecnologie, nel quale "la diminuzione dei costi di transazione nelle relazioni tra i cittadini, le formazioni sociali, gli apparati amministrativi e le istituzioni politiche apre prospettive inedite e inesplorate ai modi di funzionamento della democrazia. L'uso che della rete fatto dal movimento internazionale contro la globalizzazione dimostra che non si tratta solo di una prospettiva futuribile. Per altro verso, la nascita di comunità virtuali tematiche o territoriali, aggregate da comuni interessi e da comuni professionalità, costituirà sempre più la modalità di espressione del dibattito pubblico contribuendo a modificare l'importanza dei canali più tradizionali ivi compresi i mezzi di comunicazione di massa che oggi veicolano gran parte della comunicazione politica"[32].

Sotto il secondo profilo, quello attinente al fenomeno di deconcentrazione del potere generato dall'*eGovernment*, si assiste ad una crescente condivisione di informazione tra soggetti pubblici e tra questi ed i privati, con il conseguente affermarsi di una nuova forma di governo democratico (o *governance*), incentrata proprio sulla necessaria intensificazione di tale condivisione informativa. L'*eGovernment* diviene lo strumento trainante di tale condivisione, conducendo il sistema Italia all'*eGovernance*. L'*eGovernance* "trasforma radicalmente la logica tradizionale di funzionamento degli apparati amministrativi nella quale la rigida settorializzazione dei flussi informativi era funzionale al sistema di comando e controllo tipico delle organizzazioni gerarchiche. Ciò allarga le possibilità di decentramento e di delega dell'autorità (sia verso l'alto che verso il basso), rende

---

[30] Cfr. N. Bobbio, *L'età dei diritti*, Torino, Einaudi, 1990.

[31] Per un approfondimento della materia si rinvia a: M. Palmirani, M. Martoni (a cura di), *Il cittadino elettronico e l'identità digitale nell'eGovernance*, Bologna, Gedit Edizioni, 2006.

[32] ASTRID, *Federalismo informatico e rinnovamento delle istituzioni: dieci tesi sull'eGovernment*, p. 4, in Internet all'URL, consultato nel mese di ottobre 2009: http://www.astrid-online.it/I-paper-di/Paper-Dieci-tesi-sull-e-gov.PDF.

più labili i confini tra il settore pubblico e il resto della società, trasforma potenzialmente tutte le istituzioni in reti di organizzazioni e tutte le organizzazioni in reti di nuclei elementari. Questa tendenza alla orizzontalità, ben simboleggiata dallo sviluppo stesso di Internet, costituisce in qualche modo la base tecnologica della sussidiarietà sia verticale che orizzontale"[33]. Si palesa, dunque, il concetto di "sussidiarietà digitale", intesa come un principio politico e giuridico di vasta portata, volto ad organizzare la struttura e i rapporti tra livelli e soggetti della decisione pubblica, in modo da favorire il decentramento della decisione stessa[34].

3. La sussidiarietà digitale verticale

Il principio di sussidiarietà, inteso in senso sociale e giuridico-amministrativo, comporta l'intervento degli Enti pubblici territoriali (Regioni, Città Metropolitane, Province e Comuni), sia nei confronti dei cittadini sia degli enti e suddivisioni amministrative ad essi sottostanti, esclusivamente come sussidio (ovvero come aiuto, dal latino *subsidium*) nel caso in cui il cittadino o l'entità sottostante sia impossibilitata ad agire per conto proprio. Il medesimo principio è applicabile su scala internazionale, ovvero nel caso di 'intervento di organismi sovranazionali nei confronti degli stati membri.

Questo principio trova la propria fonte giuridica nell'articolo n. 5 del Trattato consolidato della Comunità Europea e negli articoli costituzionali nn. 2 (riconoscimento e garanzia delle formazioni sociali), 3 (partecipazione dei lavoratori all'organizzazione politica, economica e sociale del Paese), 5 (riconoscimento e promozione delle autonomie locali).

Volendo analizzare nello specifico la portata del concetto di "sussidiarietà verticale", con tale locuzione dobbiamo intendere "quel principio che informa i rapporti tra livelli diversi della deliberazione in base al quale le decisioni devono essere assunte allo stesso livello in cui esse producono i loro effetti. Ciò risponde non solo ad un principio di efficienza, per cui i soggetti, che sono confrontati ad un problema e destinati a supportare le conseguenze di una decisione, sono anche coloro ai quali dovrebbe essere attribuito il potere di decidere perché posti nella condizione migliore per valutarne le conseguenze; ma risponde anche ad un principio democratico, per cui l'analisi delle condizioni di libertà individuale in una data società o contesto deve partire dall'osservazione della possibilità che le persone hanno di progettare e realizzare davvero una vita che si possa ragionevolmente descrivere come il prodotto delle loro scelte"[35].

Il principio di sussidiarietà verticale è stato esplicitamente introdotto nella nostra Costituzione (art. 118, comma 1, nonché art. 120 comma 2)[36], a seguito della riforma del Titolo V operata

---

[33] *Ibidem*.

[34] Per un approfondimento della tematica: M. Durante, *Il futuro del web: etica, diritto, decentramento. Dalla sussidiarietà digitale all'economia dell'informazione in rete*, Torino, Giappichelli, 2007.

[35] *Ivi*, p. 235.

[36] Art. 118 Cost., comma 1: "Le funzioni amministrative sono attribuite ai Comuni salvo che, per assicurarne l'esercizio unitario, siano conferite a Province, Città metropolitane, Regioni e Stato, sulla base dei principi di sussidiarietà, differenziazione ed adeguatezza".

con Legge Costituzionale n. 3/2001.
Il principio di sussidiarietà verticale, ha assunto un'importanza essenziale nell'interpretazione delle norme costituzionali con le quali si ripartisce la competenza legislativa tra Stato e Regioni in tema di *eGovernment*. Il modello di riparto che ne scaturisce concretizza nel nostro ordinamento una forma di sussidiarietà innovativa nei caratteri e contenuti, la "sussidiarietà digitale verticale"[37].
Per comprendere appieno quanto appena detto, si consideri quanto segue.
L'art. 117 della nostra Costituzione individua le materie di competenza esclusiva legislativa dello Stato (comma 2) e quelle di competenza concorrente (comma 3) e residuale (comma 4)[38]. Tra le prime, ovvero le materie sulle quali solo lo Stato detiene il potere legislativo esclusivo e non le Regioni, rientra anche il "coordinamento informativo statistico e informatico dei dati dell'Amministrazione statale, regionale e locale" (comma 2, lett. r). Secondo un'interpretazione letterale, pertanto, l'informatica pubblica, e con essa ovviamente la realizzazione del progetto di *eGovernment*, resta un ambito decisionale rimesso in via esclusiva al legislatore statale senza alcun ruolo da parte delle autonomie locali. La Corte Costituzionale è intervenuta più volte sull'argomento, chiarendo la portata della materia ora richiamata e, dunque, la sua incidenza sulla possibilità decentrata di esercizio di potestà legislative, da parte delle Regioni, in tema di informatica pubblica.
In particolare, occorre richiamare il contenuto della sentenza n. 17/2004 del Giudice delle

Art. 120 Cost., comma 2: "Il Governo può sostituirsi a organi delle Regioni, delle Città metropolitane, delle Province e dei Comuni nel caso di mancato rispetto di norme e trattati internazionali o della normativa comunitaria oppure di pericolo grave per l'incolumità e la sicurezza pubblica, ovvero quando lo richiedono la tutela dell'unità giuridica o dell'unità economica e in particolare la tutela dei livelli essenziali delle prestazioni concernenti i diritti civili e sociali, prescindendo dai confini territoriali dei governi locali. La legge definisce le procedure atte a garantire che i poteri sostitutivi siano esercitati nel rispetto del principio di sussidiarietà e del principio di leale collaborazione".

[37] V. Sarcone, *Per un'innovazione delle politiche governative: l'eGovernment*, articolo disponibile all' URL, consultato nel mese di ottobre 2009: http://www.diritto.it/materiali/tecnologie/sarcone.html.

[38] Art. 117 Cost., commi 2, 3 e 4: "Lo Stato ha legislazione esclusiva nelle seguenti materie:
a) politica estera e rapporti internazionali dello Stato; rapporti dello Stato con l'Unione Europea; diritto di asilo e condizione giuridica dei cittadini di Stati non appartenenti all'Unione Europea;
b) immigrazione;
c) rapporti tra la Repubblica e le confessioni religiose;
d) difesa e Forze armate; sicurezza dello Stato; armi, munizioni ed esplosivi;
e) moneta, tutela del risparmio e mercati finanziari; tutela della concorrenza; sistema valutario; sistema tributario e contabile dello Stato; perequazione delle risorse finanziarie;
f) organi dello Stato e relative leggi elettorali; referendum statali; elezione del Parlamento europeo;
g) ordinamento e organizzazione amministrativa dello Stato e degli enti pubblici nazionali;
h) ordine pubblico e sicurezza, ad esclusione della polizia amministrativa locale;
i) cittadinanza, stato civile e anagrafi;

Leggi[39], in base alla quale lo spazio di intervento statale risulta alquanto limitato rispetto alla portata letterale della norma: allo Stato spetta solo un raccordo di tipo tecnico, volto ad assicurare una comunanza di linguaggi, procedure e standard omogenei su tutto il territorio nazionale, tali da rendere possibile la comunicabilità tra i vari sistemi informatici pubblici, ovvero al fine di promuovere la mera raccolta di informazioni a livello centrale[40]. Tale competenza legislativa può anche investire i profili della qualità dei servizi e della razionalizzazione della spesa in materia informatica, ma solo se ciò abbia delle conseguenze utili in termini di omogeneità nella elaborazione e trasmissione dei dati.

Considerata l'interpretazione del comma 2 lett. r) operata dalla Corte, dunque, lo Stato detiene il potere di incidere anche sull'organizzazione amministrativa regionale e degli enti locali, ma al solo scopo di dettare *standard* di interoperabilità tra i sistemi: "Laddove, invece, si esorbiti da tali spazi, con precetti che finiscano per interferire con l'organizzazione e con la dotazione strumentale delle regioni e degli enti territoriali, il principio di leale collaborazione, applicabile anche alla materia in esame, impone che venga garantito un incisivo coinvolgimento di tali enti (soprattutto il ricorso ad intese) nei procedimenti relativi alla individuazione dei mezzi informatici utili all'ammodernamento amministrativo"[41].

L'intervento della Corte, dunque, ha permesso l'effettivo avvio nel nostro paese di una pluralità di decisioni nel campo della digitalizzazione dell'apparato pubblico assunte allo

l) giurisdizione e norme processuali; ordinamento civile e penale; giustizia amministrativa;
m) determinazione dei livelli essenziali delle prestazioni concernenti i diritti civili e sociali che devono essere garantiti su tutto il territorio nazionale;
n) norme generali sull'istruzione;
o) previdenza sociale;
p) legislazione elettorale, organi di governo e funzioni fondamentali di Comuni, Province e Città metropolitane;
q) dogane, protezione dei confini nazionali e profilassi internazionale;
r) pesi, misure e determinazione del tempo; coordinamento informativo statistico e informatico dei dati dell'Amministrazione statale, regionale e locale; opere dell'ingegno;
s) tutela dell'ambiente, dell'ecosistema e dei beni culturali.

Sono materie di legislazione concorrente quelle relative a: rapporti internazionali e con l'Unione Europea delle Regioni; commercio con l'estero; tutela e sicurezza del lavoro; istruzione, salva l'autonomia delle istituzioni scolastiche e con esclusione della istruzione e della formazione professionale; professioni; ricerca scientifica e tecnologica e sostegno all'innovazione per i settori produttivi; tutela della salute; alimentazione; ordinamento sportivo; protezione civile; governo del territorio; porti e aeroporti civili; grandi reti di trasporto e di navigazione; ordinamento della comunicazione; produzione, trasporto e distribuzione nazionale dell'energia; previdenza complementare e integrativa; armonizzazione dei bilanci pubblici e coordinamento della finanza pubblica e del sistema tributario; valorizzazione dei beni culturali e ambientali e promozione e organizzazione di attività culturali; casse di risparmio, casse rurali, aziende di credito a carattere regionale; enti di credito fondiario e agrario a carattere regionale. Nelle materie di legislazione concorrente spetta alle Regioni la potestà legislativa, salvo che per la determinazione dei princìpî fondamentali, riservata alla legislazione dello Stato.

Spetta alle Regioni la potestà legislativa in riferimento ad ogni materia non espressamente riservata alla legislazione dello Stato".

[39] La sentenza C. Cost. n. 17/2004 è consultabile all'URL, visionato nel mese di ottobre 2009: http://www.cortecostituzionale.it/.

[40] A riguardo si veda C. Cost. n. 240/2007, consultabile all'URL, visionato nel mese di ottobre 2009: http://www.cortecostituzionale.it/.

[41] A.G. Orofino, *Forme elettroniche e procedimenti amministrativi*, Bari, Cacucci, 2008, p. 23. L'Autore esamina compiutamente tutte le implicazioni costituzionali connesse all'*eGovernment* e, soprattutto, alla ripartizione di competenza legislativa tra Stato e Regioni in materia (si vedano pp. 17-72). Sul punto si rimanda a C. Cost. n. 31/2005, consultabile all'URL, visionato nel mese di ottobre 2009: http://www.cortecostituzionale.it/.

stesso livello in cui esse producono i loro effetti (ad eccezione, come detto, degli standard utili all'interoperabilità), nel pieno rispetto del principio di sussidiarietà verticale.
Recentemente, con schema di Disegno di Legge del 19 febbraio 2009, recante la delega al Governo per l'adeguamento delle disposizioni in materia di enti locali alla riforma del Titolo V della parte seconda della Costituzione e per l'adozione della "Carta delle autonomie", la Presidenza del Consiglio dei Ministri ha sottolineato l'urgenza di una piena attuazione della riforma costituzionale del 2001, anche sotto il profilo della lett. r), comma 2, dell'art. 117. Il Disegno di Legge costituisce un impegno fondamentale per dare attuazione ai principî costituzionali e per giungere ad un codice chiaro e coordinato delle disposizioni riguardanti il sistema delle autonomie. In tale ottica, nell'esercizio della delega, il Governo si dovrà attenere ad una serie di criteri e indirizzi, tra i quali "prevedere strumenti idonei a garantire l'esercizio, da parte degli enti locali, di compiti conoscitivi, informativi e statistici concernenti le loro funzioni finalizzati alla circolazione delle informazioni tra Amministrazioni locali, regionali e statali, secondo standard, regole tecniche uniformi o linguaggi comuni definiti a livello nazionale, in coerenza con il quadro regolamentare europeo ed internazionale; prevedere strumenti di integrazione nel sistema informativo statistico nazionale di cui al Decreto Legislativo 6 giugno 1989, n 322, e nel sistema pubblico di connettività di cui al decreto legislativo 7 marzo 2005, n . 82"[42]. Il coordinamento delle politiche di *eGovernment*, dunque, diviene chiaramente strumento di attuazione dei principî di collaborazione e sussidiarietà tra enti. Senza tale coordinamento i futuri rapporti Stato-Enti locali rischierebbero una deriva informativo-informatica, in quanto sprovvisti di *standard* e regole tecniche uniformi.
Al di là dello strumento legislativo, nel corso del primo decennio del nuovo secolo, lo Stato e gli Enti territoriali hanno anche trovato ulteriori forme di raccordo, tali da rendere ancora più effettivo il modello di sussidiarietà digitale verticale introdotto a livello costituzionale. Si sono sviluppate, infatti, una molteplicità di strutture, inizialmente volte alla cooperazione interistituzionale nel processo di digitalizzazione pubblico ma poi, progressivamente, trasformatisi in strutture di semplice rappresentanza degli enti locali[43]. Tale ontologica trasformazione è dettata dalla difficoltà di gestione unitaria delle politiche di *eGovernment*, sviluppatesi sul territorio in modo non omogeneo, quindi con forti punte di eccellenza e altrettanto forti limiti strutturali. Un rimedio a tale situazione di caos e di scarsa razionalità nella

---

[42] Art. 4, lett. u), schema di Disegno di Legge della Presidenza del Consiglio dei Ministri del 19 febbraio 2009, recante la delega al Governo per l'adeguamento delle disposizioni in materia di enti locali alla riforma del Titolo V della parte seconda della Costituzione e per l'adozione della "Carta delle autonomie", consultabile all'URL, visionato nel mese di ottobre 2009: http://www.federalismi.it/index.cfm?nrS=142.

[43] Una compiuta elencazione di tali strutture è effettuata da R. De Rosa, *Il cuore del governo elettronico*, in "Polis", n. 1, 2007, p. 112, nota 36: Commissioni permanenti per l'innovazione e le tecnologie, Tavolo congiunto permanente, Commissione di coordinamento del sistema pubblico di connettività, Cabina di regia del sistema informativo sanitario, Tavolo di lavoro permanente per la sanità elettronica, Comitato tecnico della commissione permanente per l'innovazione e le tecnologie nelle regioni, Intesa tra Stato, regioni ed enti locali sui sistemi informativi geografici, Comitato per le regole tecniche sui dati territoriali delle Pubbliche Amministrazioni, Tavolo di coordinamento per il sistema informativo ambientale, Tavolo tecnico permanente per il sistema informativo del lavoro, Comitato nazionale sul turismo, Comitato tecnico per la sperimentazione della carta d'identità elettronica, Comitati di coordinamento tra le Regioni e gli enti locali del territorio per lo sviluppo dei piani regionali per la Società dell'informazione, Centri regionali di competenza per l'*eGovernment* e la Società dell'informazione, Agenzia per la diffusione delle tecnologie per l'innovazione.

governance, si è avuta con l'avvio nel 2006 dei lavori della Commissione permanente unificata per l'innovazione tecnologica nelle Regioni e negli Enti Locali, prevista dall'art. 14 del CAD e l'avvio di una più generale ricognizione degli organismi di cooperazione operanti fra centro e periferia, facilitando in tal modo una piena realizzazione del principio di sussidiarietà verticale in campo di *eGovernment*.

Tale principio, però, necessita non solo di strumenti politico-normativi per la sua piena realizzazione ma anche di concreti strumenti tecnico-informatici. Nell'ottica di sussidiarietà verticale, infatti, occorre fornire alle Amministrazioni locali gli strumenti per meglio operare e collegarsi tra loro e con le istituzioni centrali, consentendo alle stesse di erogare servizi di *front-office* qualitativamente migliori e senza il bisogno di operatori interposti tra amministratore e utente, nonché agli uffici di *back-office* di poter operare in maniera più produttiva e funzionale, grazie ad una comunicazione interna assistita dalle procedure informatiche. Gli strumenti tecnico-informatici più efficaci a tali fini sono stati individuati nelle Reti informatiche pubbliche. Queste Reti, infatti, intendono permettere, nella quotidianità, un interscambio di dati tra Amministrazioni, necessario per un ottimale svolgimento di un'attività decisionale decentrata.

Il primo progetto di Rete informatica pubblica è rappresentato dalla Rete Unitaria per la Pubblica Amministrazione (RUPA): esso coincide con l'istituzione presso l'AIPA, nel 1997, del Centro Tecnico della Rete Unitaria, ma la sua operatività la si può far risalire al marzo del 2000.

La RUPA rappresenta l'organizzazione delle risorse intangibili (informatiche, tecnologiche e di comunicazione) degli apparati pubblici, al fine di consentire l'interconnessione, mediante la rete dei Domini delle singole Amministrazioni, con il Dominio della Rete Unitaria, permettendo la interoperabilità tra le diverse Amministrazioni per l'accesso ai relativi servizi[44].

Quindi, gli utenti dei servizi offerti dal "progetto" sono sostanzialmente:

- le Amministrazioni Centrali e gli Enti Pubblici non economici[45];
- le Amministrazioni che hanno la facoltà di avvalersi dei servizi[46];
- i soggetti che aggregano più Amministrazioni Locali (con facoltà di avvalersi dei servizi), limitatamente ai collegamenti con le altre Amministrazioni appartenenti al dominio della RUPA.

I servizi previsti consistono, sostanzialmente, nella interconnessione a livello applicativo tra gli apparati e comprendono l'accesso al *web*, il trasferimento di *file*, la posta elettronica, il terminale virtuale, il *domain name service*, la *directory service*, il *system management and network*, il *call center*, la formazione.

Nel 2007, a seguito della scadenza del contratto RUPA, il progetto è confluito nell'ambito di un sistema ancora più ampio e complesso, ossia il Sistema Pubblico di Connettività (SPC), che, secondo taluni, ha ereditato le criticità tecnico-organizzative della RUPA[47]. L'SPC, in base all'art.

---

[44] Cfr. C. Rabbito, *L'informatica al servizio della Pubblica Amministrazione e del cittadino*, cit., pp. 159-162.

[45] Amministrazioni ed Enti pubblici non economici come individuati all'art. 1, comma 1, del D.Lgs. n. 39/1993.

[46] Si intendono quelle diverse dall'elenco previsto dall'art. 1 del D.Lgs. n. 39/1993.

[47] Cfr. A. Natalini, *Il Sistema Pubblico di Connettività. Il SPC: eredita i problemi della RUPA*, in "Giornale di Diritto Amministrativo", n. 7, 2005, pp. 702-707; E. Belisario, *Il Sistema Pubblico di Connettività*, in Quaranta M. (a cura di), *Il*

73 del Codice dell'Amministrazione Digitale (CAD), può essere definito come "l'insieme di infrastrutture tecnologiche e di regole tecniche, per lo sviluppo, la condivisione, l'integrazione e la diffusione del patrimonio informativo e dei dati della Pubblica Amministrazione, necessarie per assicurare l'interoperabilità di base ed evoluta e la cooperazione applicativa dei sistemi informatici e dei flussi informativi, garantendo la sicurezza, la riservatezza delle informazioni, nonché la salvaguardia e l'autonomia del patrimonio informativo di ciascuna Pubblica Amministrazione".

All'interno della citata norma, bisogna intendere per:

- "trasporto di dati" i servizi per la realizzazione, gestione ed evoluzione di reti informatiche per la trasmissione di dati, oggetti multimediali e fonia;
- "interoperabilità di base" i servizi per la realizzazione, gestione ed evoluzione di strumenti per lo scambio di documenti informatici fra le Pubbliche Amministrazioni e tra queste e i cittadini;
- "connettività" l'insieme dei servizi di trasporto di dati e di interoperabilità di base;
- "interoperabilità evoluta" i servizi idonei a favorire la circolazione, lo scambio di dati e informazioni e l'erogazione fra le Pubbliche Amministrazioni e tra queste e i cittadini;
- "cooperazione applicativa" la parte del SPC finalizzata all'interazione tra i sistemi informatici delle Pubbliche Amministrazioni per garantire l'integrazione dei metadati, delle informazioni e dei procedimenti amministrativi[48].

Tale disciplina è applicabile a tutte le Pubbliche Amministrazioni di cui all'art. 1, comma 2, del D.Lgs. n. 165/2001[49], a meno che non sia diversamente stabilito dalla legge, sempre comunque nel rispetto della loro autonomia organizzativa e del riparto di competenza di cui all'art. 117 della Costituzione.

Affiancato al progetto SPC si trova il progetto RIPA (Rete Internazionale delle Pubbliche Amministrazioni), avente il fine di collegare tramite la rete le sedi estere della Pubblica Amministrazione, con modalità improntate su principî di sicurezza informatica ed in maniera efficiente in termini di fruizione dei servizi, quali ad esempio: l'anagrafe consolare *online*, il sistema delle votazioni per gli italiani residenti all'estero, il procedimento dei visti e lo sportello unico per gli italiani che vivono in paesi stranieri.

Attraverso la RIPA, dunque, l'essenza della sussidiarietà verticale, ovvero la necessità di decisioni assunte allo stesso livello in cui esse producono i loro effetti, travalica gli stessi confini nazionali, assumendo un innovativo profilo internazionale se non, addirittura, globale.

Codice della Pubblica Amministrazione Digitale, Napoli, Liguori Editore, 2006, pp. 229-250; C. D'Orta, *Il Sistema Pubblico di Connettività. Il SPC: un approccio nuovo alle esigenze della rete delle Pubbliche Amministrazioni*, in "Giornale di Diritto Amministrativo", n. 7, 2005, pp. 693-702.

[48] Cfr. Riem G., *Sistema Pubblico di Connettività*, in Borruso R., Riem G., Sirotti Gaudenzi A., Vicenzotto P. (a cura di), *Glossario di diritto delle nuove tecnologie e dell'e-government*, Milano, A. Giuffré Editore, 2007, pp. 460-463.

[49] In base alla norma citata, si devono intendere per "Amministrazioni Pubbliche" tutte le Amministrazioni dello Stato, ivi compresi gli istituti e scuole di ogni ordine e grado e le istituzioni educative, le aziende ed Amministrazioni dello Stato ad ordinamento autonomo, le Regioni, le Province, i Comuni, le Comunità montane, e loro consorzi e associazioni, le istituzioni universitarie, gli Istituti autonomi case popolari, le Camere di commercio, industria, artigianato e agricoltura e loro associazioni, tutti gli enti pubblici non economici nazionali, regionali e locali, le Amministrazioni, le aziende e gli enti del Servizio sanitario nazionale, l'Agenzia per la rappresentanza negoziale delle Pubbliche Amministrazioni (ARAN) e le Agenzie di cui al D.Lgs. n. 300/1999.

Considerati gli strumenti rappresentati dal SPC e dalla RIPA, associati all'ambito di intervento normativo riservato dalla Corte Costituzionale alle Regioni in base all'art. 117, comma 2, lett. r), ed ai vari tavoli di concertazione e coordinamento interistituzionali in tema di *eGovernment*, appare chiara la scelta del legislatore italiano di intraprendere la strada del "federalismo informatico", già espressamente indicata nel 2003 dal Ministro Lucio Stanca[50].
Il "federalismo informatico", o "governo federato dell'informatica pubblica"[51], appare dunque come un logico corollario della visione del nostro Stato come uno "Stato diffuso", comunitario, per la sua forte configurazione pluralistica[52] o, secondo altri, corollario della concezione dello "Stato a rete", in quanto caratterizzato dalla sua forte dimensione relazionale tra Enti[53]. Lo Stato, in definitiva, con l'avvento dell'*eGovernment*, diviene uno "Stato virtuale", o *Virtual State*, ovvero un governo organizzato in modo crescente in termini di agenzie virtuali e network pubblico-privati, la cui struttura e capacità dipendono da internet e dal *web*[54] e nel quale i confini delle Amministrazioni perdono gran parte del loro tradizionale carattere territoriale, generando il fenomeno della "virtualizzazione delle comunità di riferimento"[55].

4. La sussidiarietà digitale orizzontale

Volendo ora analizzare nello specifico la portata del concetto di "sussidiarietà orizzontale", con tale locuzione dobbiamo intendere "quel principio in base al quale è necessario favorire l'autonoma iniziativa degli individui, singoli e associati, per il compimento d'attività d'interesse comune. La realizzazione di un interesse o bene comune non dipende, in questa prospettiva, da una programmazione centralizzata, che assegni ad ogni individuo un ruolo o un compito specifici, quanto piuttosto dall'interazione di una molteplicità d'individui"[56].
Anche il principio di sussidiarietà orizzontale, al pari di quello di sussidiarietà verticale, è stato esplicitamente introdotto nella nostra Costituzione (artt. 118, comma 4)[57], a seguito della riforma del Titolo V operata con Legge Costituzionale n. 3/2001.
Le politiche di *eGovernment* attuate negli ultimo decennio nel nostro paese si sono caratterizzate per la loro "cittadino-centricità", ovvero il posizionamento del cittadino al centro dell'attenzione del legislatore: "cittadino al centro è un modo di essere della Pubblica Amministrazione che

---

50 Cfr. E. Grazzini, *Federalismo in versione hi-tech*, in "Corriere della Sera-Corriere Economia", 7 aprile 2003, p. 11.

51 R. De Rosa, *Il cuore del governo elettronico*, op. cit., p. 114.

52 Cfr. I. Diamanti, *Il ritorno dello Stato. L'Italia, dal regionalismo al neocentralismo*, in P. Messina (a cura di), *Sistemi locali e spazio europeo*, Roma, Carocci, 2003, pp. 228-245; J.E.Fountain, *Building the Virtual State: Information Technology and Institutional Change*, Harward, Brookings Institution, 2001.

53 Cfr. M. Castells, *Galassia Internet*, Milano, Feltrinelli, 2002.

54 Cfr. J. Fountain, *Building the Virtual State: Information Technology and Institutional Change*, op. cit..

55 L. Buccoliero, *Il governo elettronico*, op. cit., p. 10.

56 M. Durante, *Il futuro del web: etica, diritto, decentramento. Dalla sussidiarietà digitale all'economia dell'informazione in rete*, op. cit., p. 235.

57 Art. 118 Cost., comma 4: "Stato, Regioni, Città metropolitane, Province e Comuni favoriscono l'autonoma iniziativa dei cittadini, singoli e associati, per lo svolgimento di attività di interesse generale, sulla base del principio di sussidiarietà".

fornisce servizi utili, efficienti e personalizzati per il singolo cittadino, in grado di aprire il dialogo democratico e di valorizzare le capacità di ascolto"[58]. La sussidiarietà orizzontale, attraverso un percorso "cittadino-centrico", diviene quindi sussidiarietà digitale orizzontale, perché la partecipazione attiva dei cittadini ai procedimenti amministrativi, attuabile grazie all'interconnessione telematica di questi con le Amministrazioni, consente ai privati di gestire direttamente alcune delle procedure amministrative prima bisognose di appositi uffici ed operatori per il ricevimento delle istanze da parte del pubblico[59]. La partecipazione del cittadino ai procedimenti amministrativi con l'ausilio delle nuove tecnologie, peraltro, ha costituito oggetto dell'art. 9 del CAD, intitolato "Partecipazione democratica elettronica", nel quale si legge: "Lo Stato favorisce ogni forma di uso delle nuove tecnologie per promuovere una maggiore partecipazione dei cittadini, anche residenti all'estero, al processo democratico e per facilitare l'esercizio dei diritti politici e civili sia individuali che collettivi".
Si attua in tal modo la "*eParticipation*", ovvero l'uso di informazioni e tecnologie di comunicazione per ampliare ed approfondire la partecipazione politica, abilitando i cittadini alla connessione reciproca e con i loro rappresentanti eletti[60]. L'*eParticipation* si pone, dunque, come specificazione dell'*eDemocracy*, da intendersi quest'ultima, come già detto[61], quale insieme delle attività attraverso le quali il Governo raccoglie le opinioni dei cittadini e delle imprese su un ampio numero di materie, dal cambiamento di leggi e regolamenti alla modifica di aspetti gestionali di specifici programmi e servizi. L'*eParticipation*, pertanto, rafforza la natura stessa dell'*eDemocracy*, affermatisi quale "risposta all'esigenza delle Amministrazioni di far fronte alla crescente complessità delle decisioni mediante un coinvolgimento più ampio delle competenze e delle esperienze diffuse nella società"[62].
L'Unione Europea ha avviato uno specifico programma definito "*eParticipation preparatory action*", di durata triennale (2006-2008), volto a dimostrare come l'utilizzo delle ICT può rendere più semplice la partecipazione dei cittadini alle fasi decisionali pubbliche e contribuire ad una migliore legislazione, soprattutto consentendo un più facile accesso alle proposte di legge ed un'espressione di opinione. L'azione è stata iniziata dal Parlamento europeo nel 2006[63] ed ha sostenuto nel tempo una serie di progetti di pilota. Nel gennaio del 2008 è stato poi avviato dalla Commissione Europea il progetto "*European eParticipation*", conclusosi nel

---

[58] A. Romano, L. Marasso, M. Marinazzo, *Italia chiama eGovernment*, op. cit., p. 127. Per un approfondimento della portata del neologismo "*citizen-centricity*" e della sua genesi in ambito europeo, si rinvia a CCegov Organizational change for citizen centric eGovernment, *A Handbook for Citizen-centric eGovernment, Version 2.1*, eGovernment unit, DG Information Society and Media, European Commission, 2007 consultabile all'URL, visionato nel mese di ottobre 2009: http://www.ccegov.eu/downloads/Handbook_Final_031207.pdf.

[59] V. Sarcone, *Per un'innovazione delle politiche governative: l'eGovernemnt*, op. cit..

[60] Cfr. A. Macintosh, *eParticipation in policy-making: the research and the challenge*s, Amsterdam, IOS Press, 2006.

[61] Si veda il primo paragrafo.

[62] C. Rabbito, *Il percorso di attuazione dell'eGovernment nella Pubblica Amministrazione italiana*, op. cit., p. 45. Strettamente connesso al tema dell'*eDemocracy* e dell'*eParticipation* è quello della "cittadinanza elettronica", per il quale si rimanda a: E. Di Maria, S. Micelli, *Le frontiere dell'e-government: cittadinanza elettronica e riorganizzazione dei servizi in rete,* Franco Angeli, Milano, 2004.

[63] Per un costante aggiornamento dell'avanzamento delle politiche europee in tema di *eParticipation* si consulti l'URL, visionato nel mese di ottobre 2009: http://ec.europa.eu/information_society/activities/egovernment/implementation/prep_action/index_en.htm.

giugno 2009, volto a permettere uno *screening* delle esperienze europee di settore, al fine di evidenziare *best practices*[64].

In Italia, nell'ottica di una piena attuazione del principio di sussidiarietà orizzontale, ovvero il favorire l'autonoma iniziativa degli individui, singoli e associati, per il compimento d'attività d'interesse comune, particolarmente interessante risultano taluni Obiettivi fissati dal Piano di *eGovernment* 2012[65], emanato nel dicembre 2008 dal Ministro Brunetta che, partendo dalla Direttiva del Dipartimento per l'Innovazione e le Tecnologie dal Ministro Stanca nel 2005, incentrata sulla necessità di estensione dei servizi online al cittadino, qualità dell'Amministrazione Pubblica e *customer satisfaction* del cittadino/cliente, fa leva sull'attuazione del Codice dell'Amministrazione Digitale e del Piano Industriale della Pubblica Amministrazione del maggio 2008[66].

L'Obiettivo n. 8, intitolato "Ambiente", in particolare, è finalizzato a rendere disponibile *online* il patrimonio dei dati ambientali e geografici (zone protette e aree vincolate, ortofoto e modello digitale del terreno ad altissima risoluzione, analisi sul territorio, dati di monitoraggio) curati dal Ministero dell'Ambiente per scopi di studio (dalle elementari all'università), ma anche per le attività amministrative e commerciali, attraverso una più sistematica e razionale organizzazione dei sistemi esistenti (razionalizzare collegamenti e flussi per lo scambio dei dati tra soggetti pubblici nel contesto della cooperazione applicativa del SPC; uniformare i dati e la loro presentazione sui siti). Consentire una trasparenza ambientale significa ovviamente dotare i cittadini e le loro associazioni degli strumenti più utili per una concreta lotta a fenomeni radicati sul territorio italiano, come l'abusivismo edilizio o la creazione di discariche di rifiuti abusive. In definitiva, significa facilitare, secondo uno schema di sussidiarietà orizzontale, il compimento d'attività d'interesse comune, poiché comune è l'ambiente e il problema della sua salvaguardia.

Sul medesimo piano, l'Obiettivo n. 10, intitolato "Beni culturali", è anche diretto alla realizzazione del "Progetto CulturAmica - Portale della Cultura", volto a rendere accessibile il vasto patrimonio di risorse e documenti, provenienti da archivi, musei, biblioteche, fondazioni, regioni, enti locali, altri enti pubblici e privati dei vari settori della cultura italiana, descrivendone le informazioni secondo una classificazione comune e condivisa. Anche in tal caso, una trasparenza nella gestione del patrimonio culturale equivale a facilitare lo svolgimento da parte dei cittadini, o associazioni di essi, di attività di interesse comune.

Infine, è da ricordare nell'ambito dell'Obiettivo n. 11, intitolato "Gioventù, Pari opportunità e Affari sociali", il "Progetto Laboratori informatici in Rete" destinato a mettere a disposizione dei giovani, in aree di particolare disagio sociale, una rete di 200 laboratori informatici, attrezzati con *personal computer*, programmi *software* avanzati, tecnologie multimediali e collegamenti veloci a Internet, al fine di prevenire e contrastare le condizioni del disagio giovanile, soprattutto in relazione al fenomeno dell'abbandono scolastico e al pericolo di devianza, con un intervento mirato all'aggregazione, all'accesso e all'utilizzo delle tecnologie ICT, in un'ottica di educazione

---

[64] Per un approfondimento si rimanda all'URL, visionato nel mese di ottobre 2009: http://www.european-eparticipation.eu/index.php?option=com_content&task=view&id=14&Itemid=31.

[65] Si veda quanto detto riguardo al Piano di *eGovernment* 2012 nel primo paragrafo.

[66] Il Piano di *eGovernment* 2012 e il Piano Industriale della Pubblica Amministrazione sono consultabili all'URL, consultato nel mese di ottobre 2009: http://www.funzionepubblica.it/home.htm.

alla legalità, di valorizzazione delle competenze e di formazione al mondo del lavoro. Anche tale progetto, rappresenta un chiaro esempio di come l'*eGovernment* possa andare incontro al tessuto territoriale, favorendone un autonomo sviluppo e un'autonoma partecipazione, nel medio termine, a processi decisionali pubblici più sentiti e condivisi. Permettere a giovani in condizione di disagio di crescere e inserirsi nella Rete Internet, che sempre più rappresenta il vivere globale, significa formarli in vista di una consapevole partecipazione democratica da adulti, sostenendo al contempo la democrazia e l'inclusione informatica.

L'inclusione informatica, anche detta *eInclusion*, diviene dunque anche nei Piani nazionali, dopo la sua affermazione a livello europeo con l'Agenda di Lisbona e l'iniziativa i2010 "Società europea dell'informazione per la crescita e l'occupazione"[67], un obiettivo essenziale dello Stato e uno strumento stesso di facilitazione alla sussidiarietà. L'*eInclusion*, infatti, fa riferimento alle azioni per realizzare una Società dell'Informazione "inclusiva", ossia una Società dell'Informazione per tutti. L'obiettivo è consentire, a tutti coloro che lo desiderano, di partecipare a pieno titolo alla Società dell'Informazione, anche se si trovano in situazioni di svantaggio sociale o personale. Superare il *digital divide*, ovvero il divario digitale, esistente tra la categoria di cittadini in grado di utilizzare al meglio gli strumenti offerti dalle ICT e la categoria di cittadini non preparati ad essi, significa non solo elevare qualitativamente la forza lavoro, ma anche rafforzare nel medio termine la partecipazione democratica. È lecito pensare, infatti, che nell'arco di un decennio l'informatica avrà un ruolo di rilievo nel rapporto quotidiano cittadino-Amministrazione e che la maggioranza dei processi burocratici sarà gestibile *online*: permettere l'inclusione informatica oggi significa, pertanto, permettere allo stesso principio di sussidiarietà orizzontale di divenire nel medio termine non solo effettivo ma facilmente applicabile nel vivere quotidiano. Di questo, peraltro, è consapevole lo stesso legislatore nazionale, il quale, all'art. 8 del CAD, intitolato "Alfabetizzazione informatica dei cittadini", dispone: "Lo Stato promuove iniziative volte a favorire l'alfabetizzazione informatica dei cittadini con particolare riguardo alle categorie a rischio di esclusione, anche al fine di favorire l'utilizzo dei servizi telematici delle Pubbliche Amministrazioni". Si palesa, pertanto, la natura delle politiche di *eInclusion* come politiche sussidiarie rientranti nel più vasto processo di *eDemocracy*.

Ma le politiche di *eGovernment* ed *eDemocracy* non detengono solo aspetti positivi, sussistono, infatti, delle zone d'ombra. Nonostante l'enorme sforzo sinora profuso dall'Unione Europea e dallo Stato in tema di *eGovernment* ed *eDemocracy*, sono da condividere talune riflessioni critiche secondo le quali "a fronte dei suoi innegabili vantaggi, la diffusione crescente delle nuove tecnologie comporta anche pesanti ricadute in termini di legittimità democratica, giustificando le preoccupazioni di quanti descrivono la resa della politica alla tecnologia. La storia recente del nostro paese mostra come la tecnologia possa costituire un'arma a doppio taglio: promuove la partecipazione ma può essere anche artefice di esclusione, favorisce la

---

[67] Cfr. Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni dell'8 novembre 2007, *Iniziativa europea i2010 sull'eInclusione "Partecipare alla società dell'informazione"*, consultabile all'URL, visionato nel mese di ottobre 2009: http://ec.europa.eu/information_society/activities/einclusion/docs/i2010_initiative/comm_native_com_2007_0694_f_it_acte.pdf.

trasparenza dei processi ma, al tempo stesso, è uno strumento di controllo dei cittadini" [68].
Il rischio è che la politica di *eGoverment*, e con essa quella più specifica di partecipazione elettronica, si possa rivelare nel tempo una pura "politica simbolica", ovvero una politica caratterizzata da un forte divario tra l'ambizione dei programmi e le decisioni effettive, con una voluta discrepanza fra l'aspettativa di *policy* (simbolo) e la loro portata effettiva (contenuto)[69].
Classico esempio in Italia di tale discrepanza è rappresentato dal contenuto dell'art. 3 del CAD[70]. Tale norma, come più volte richiamato, riconosce in capo a cittadini e imprese il diritto all'uso delle tecnologie telematiche nelle comunicazioni con le Pubbliche Amministrazioni. Ma tale diritto appare tale solo sulla carta. Infatti, non solo ad oggi non vi è stata alcuna pronuncia giudiziaria volta a tutelarlo, ma la più attenta dottrina ha messo giustamente in rilievo come tale diritto soggettivo sia tale sono nei confronti delle Pubbliche Amministrazioni statali, divenendo invece mero interesse legittimo, con una diversa e probabilmente più debole forza giuridica, nei confronti delle Amministrazioni regionali e locali[71]. Un differente grado di tutela che comporta, appunto, una forte discrepanza tra l'ambizione del programma legislativo iniziale, volto a riconoscere un diritto universale all'uso delle tecnologie nei confronti dell'intera Pubblica Amministrazione, e la sua portata effettiva.
Il superamento di queste politiche simboliche connesse all'uso della tecnologia potrà avvenire, per assurdo, solo attraverso l'introduzione di ulteriore tecnologia, in grado di

---

[68] M. Zuccarini, *Dieci anni di governo elettronico in Italia: destra e sinistra a confronto*, in "Polis", n. 1, 2007, p. 29. L'Autrice condivide, sostanzialmente, le tesi espresse da D. Carter, *Digital Democracy or Information Aristocracy?, in B.D. Loader, The Governance of Cyberspace*, Routledge, London, 1997, pp. 137-152.
Un tema interessante connesso alla partecipazione elettronica, alla trasparenza dei processi e alle forme di controllo sul cittadino è quello dell'etica informatica, pregevolmente sviluppato nello scritto: G. Ziccardi, *Etica e Informatica*, Milano, Pearson Paravia Bruno Mondadori, 2009.

[69] F. Musella, *Quale politica per il governo elettronico in Italia: costitutiva, distributiva o simbolica?*, in "Polis", n. 1, 2007, pp. 31-51. Accanto alla dimensione simbolica delle politiche di *eGovernment*, l'Autore analizza anche il profilo costitutivo (connesso all'innovazione amministrativa introdotta dall'*eGovernment*) e distributivo delle stesse (connesso all'allocazione delle risorse in ambito territoriale per lo sviluppo dell'*eGovernment*).

[70] Per il contenuto dell'art. 3 CAD si veda la nota n. 12.

[71] Cfr. A. Cacciari, *Commento art. 3 CAD* in M. Atelli, S. Aterno, A. Cacciari, R. Cauteruccio, *Codice dell'Amministrazione Digitale: commentario*, op. cit., pp. 18-22. L'Autore giustamente evidenzia come "il diritto all'uso delle tecnologie telematiche nelle comunicazioni con le Pubbliche Amministrazioni costituisce espressione del principio di buon andamento dell'attività amministrativa di cui all'art. 97 Cost., e pertanto si può ritenere che sia costituzionalmente protetto. Ma se così è, riesce allora difficile comprendere quanto dispone il comma 1-bis dell'articolo in commento, che subordina l'applicazione di quello che definisce non più un diritto ma un principio […] nei confronti delle Amministrazioni regionali e locali alla disponibilità di adeguate risorse tecnologiche ed organizzative, e prevede anche che venga rispettata, nell'applicazione di tale principio, la loro autonomia normativa. In questo modo quello che è un diritto costituzionalmente protetto si trasforma in interesse legittimo, subordinato alla disponibilità di adeguate risorse da parte degli Enti" (*Ivi*, p. 21).
La Sezione Consultiva per gli atti normativi del Consiglio di Stato n. 11995/2005, commentando lo schema di decreto legislativo recante il CAD, ha assunto posizioni ancor più drastiche sulla portata dell'art. 3 CAD. Il Consiglio di Stato, infatti, ha ritenuto che la posizione tutelata dall'art. 3 debba configurarsi, sia nei confronti delle Pubbliche Amministrazioni statali che riguardo le Amministrazioni regionali e locali, come un puro interesse legittimo, in quanto la potestà organizzatoria della Pubblica Amministrazione, nel caso in questione esercitata nel decidere i mezzi tecnici utili a garantire il colloquio telematico, è da ritenersi esercizio di potestà autoritativa, a fronte del quale non può che sussistere una mera situazione di interesse legittimo in capo al cittadino. Per un approfondimento si consulti: A. Cacciari, *Commento art. 3 CAD* in M. Atelli, S. Aterno, A. Cacciari, R. Cauteruccio, *Codice dell'Amministrazione Digitale: commentario*, op. cit., pp. 18-22; A.G. Orofino, *Forme elettroniche e procedimenti amministrativi*, op. cit., pp. 144-147.

sopperire alle mancanze oggi evidenziate nell'*eDemocracy*. Solo l'evoluzione delle ICT, infatti, potrà permettere che il simbolo diventi contenuto, che l'innovazione rafforzi la legittimità democratica, ovvero la ripartizione equilibrata dei poteri affidati alle istituzioni europee e nazionali, tramite il coinvolgimento diretto dei cittadini e dei Parlamenti nazionali al processo decisionale. La via da seguire in termini di ICT applicate all'Amministrazione è quella della multicanalità e multimedialità. Infatti, secondo un'accorta analisi di mercato, si ritiene che l'*eGovernment* evolverà a breve verso le nuove forme di *tGovernment* e *mGovernment*, volendo rappresentare con il primo termine (*tGovernment*) il sempre più massiccio utilizzo del digitale terrestre come strumento di comunicazione ed interazione con il cittadino, e con il secondo (*mGovernment*) i servizi pubblici erogati con modalità di telefonia mobile[72]. La sicura riferibilità di atti e dati trasmessi o richiesti tramite queste nuove forme di interrelazione sarà assicurata, poi, dall'implementazione dei sistemi biometrici, ove per biometria (dalle parole greche *bìos* = "vita" e *metros* = "conteggio" o "misura") dobbiamo intendere la scienza che ha come oggetto di studio la misurazione delle variabili fisiologiche o comportamentali tipiche degli organismi, attraverso metodologie matematiche e statistiche. I dati biometrici di un essere umano sono derivabili dalla misurazione di varie caratteristiche del corpo o del comportamento (impronte digitali, iride, ecc.) e possono essere utilizzati a fini identificativi[73]. Si pensi, ad esempio, ai progetti in tema di *eVoting*, ovvero il voto elettronico, in base ai quali in un prossimo futuro il cittadino sarà in grado di esprimere il proprio giudizio elettorale direttamente dalla propria abitazione, munito di connessione alla Rete Internet e di un apposito apparecchio in grado di identificarlo in base a dati biometrici[74].
Non ci resta che attendere, sperando che tali novità favoriscano sempre più l'autonoma iniziativa degli individui, singoli e associati, per il compimento d'attività d'interesse comune.

BIBLIOGRAFIA

Assar S., Boughzala I. (a cura di), *Administration électronique: constats et perspectives*, Paris, GET et Lavoisier, 2007.
ASTRID, *Federalismo informatico e rinnovamento delle istituzioni: dieci tesi sull'eGovernment*, in Internet all'URL, consultato nel mese di ottobre 2009: http://www.astrid-online.it/I-paper-di/Paper-Dieci-tesi-sull-e-gov.PDF.
Atelli M., Aterno S., Cacciari A., Cauteruccio R., *Codice dell'Amministrazione Digitale: commentario*, Roma, Istituto Poligrafico e Zecca dello Stato, 2008.
Belisario E., *Il Sistema Pubblico di Connettività*, in Quaranta M. (a cura di), *Il Codice della Pubblica Amministrazione Digitale*, Napoli, Liguori Editore, 2006.

[72] Cfr. P. Giacalone, *La normativa sul governo elettronico*, op. cit..

[73] Una compiuta analisi della normativa nazionale ed internazionale in tema di biometria è svolta in: G. Preite, *Il riconoscimento biometrico. Sicurezza versus privacy*, Trento, UniService, 2007.

[74] Particolarmente interessante, in quanto rappresentativo anche delle sperimentazioni ed iniziative in atto, è l'approfondimento in tema di biometria effettuato dal CNIPA all'URL, consultato nel mese di ottobre 2009: http://www.cnipa.gov.it/site/it-IT/Attivit%c3%a0/Tecnologie_innovative_per_la_PA/Biometria/.

Id., *La nuova Pubblica Amministrazione Digitale*, Santarcangelo di Romagna, Maggioli Editore, 2009.
Bell D., *The coming of post-industrial society*, New York, Basic Books, 1973.
Bobbio N., *L'età dei diritti*, Torino, Einaudi, 1990.
Buccoliero L., *Il governo elettronico*, Milano, Tecniche Nuove, 2009.
Cacciari A., *Commento art. 3 CAD*, in Atelli M., Aterno S., Cacciari A., Cauteruccio R., *Codice dell'Amministrazione Digitale: commentario*, op. cit..
Cacciari A., *Commento art. 9 CAD* in Atelli M., Aterno S., Cacciari A., Cauteruccio R., *Codice dell'Amministrazione Digitale: commentario*, op. cit..
Caldow J., *The quest for electronic government: a defining vision*, Washington DC, Institute for Electronic Government, 1999.
Carter D., *Digital Democracy or Information Aristocracy?, in B.D. Loader, The Governance of Cyberspace*, Routledge, London, 1997.
Castells M., *End of millenium*, Oxford, Maldel, 2000.
Castells M., *Galassia Internet*, Feltrinelli, Milano, 2002.
CCegov Organizational change for citizen centric eGovernment, *A Handbook for Citizen-centric eGovernment, Version 2.1*, eGovernment unit, DG Information Society and Media, European Commission, 2007 consultabile all'URL, visionato nel mese di ottobre 2009: http://www.ccegov.eu/downloads/Handbook_Final_031207.pdf.
Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, *Iniziativa europea i2010 sull'eInclusione "Partecipare alla società dell'informazione"*, consultabile all'URL, visionato nel mese di ottobre 2009: http://ec.europa.eu/information_society/activities/einclusion/docs/i2010_initiative/comm_native_com_2007_0694_f_it_acte.pdf.
Contaldo A., *Dalla teleamministrazione all'e-government: una complessa transizione in fieri*, in "Foro Amministrativo", n. 4, 2002.
D'Avanzo W., *L'e-government*, MoviMedia, Lecce, 2007.
De Rosa R., *Il cuore del governo elettronico*, in "Polis", n. 1, 2007.
Diamanti I., *Il ritorno dello Stato. L'Italia, dal regionalismo al neocentralismo*, in Messina P. (a cura di), *Sistemi locali e spazio europeo*, Roma, Carocci, 2003.
Di Maria E., Micelli S., *Le frontiere dell'e-government: cittadinanza elettronica e riorganizzazione dei servizi in rete,* FrancoAngeli, Milano, 2004.
D'Orta C., *Il Sistema Pubblico di Connettività. Il SPC: un approccio nuovo alle esigenze della rete delle Pubbliche Amministrazioni*, in "Giornale di Diritto Amministrativo", n. 7, 2005.
Duni G., *Teleamministrazione* (voce), in *Enciclopedia Giuridica Treccani*, Roma, XXX, n. 5, 1993.
Durante M., *Il futuro del web: etica, diritto, decentramento. Dalla sussidiarietà digitale all'economia dell'informazione in rete*, Torino, Giappichelli, 2007.
Fountain J.E., *Building the Virtual State: Information Technology and Institutional Change*, Harward, Brookings Institution, 2001.
Giacalone P., *La normativa sul governo elettronico*, Milano, Franco Angeli, 2007.
Grazzini E., *Federalismo in versione hi-tech*, in "Corriere della Sera-Corriere Economia", 7 aprile 2003.
Holmes D., *Egov: E-Business strategies for government*, London, Nicholas Brealey Publishing, 2001.
Macintosh A., *eParticipation in policy-making: the research and the challenge*s, Amsterdam, IOS Press, 2006.
Merloni F. (a cura di), *Introduzione all'eGovernment*, Torino, Giappichelli, 2005.

Musella F., *Quale politica per il governo elettronico in Italia: costitutiva, distributiva o simbolica?*, in "Polis", n. 1, 2007.
Natalini A., *Il Sistema Pubblico di Connettività. Il SPC: eredita i problemi della RUPA*, in "Giornale di Diritto Amministrativo", n. 7, 2005.
Orofino A.G., *Forme elettroniche e procedimenti amministrativi*, Bari, Cacucci, 2008.
Palmirani M., Martoni M. (a cura di), *Il cittadino elettronico e l'identità digitale nell'eGovernance*, Bologna, Gedit Edizioni, 2006.
Preite G., *Il riconoscimento biometrico. Sicurezza versus privacy*, Trento, UniService, 2008.
Presidenza Consiglio dei Ministri-Dipartimento della Funzione Pubblica, *eGovernment e organizzazione nelle Amministrazioni Pubbliche. Analisi di caso sulle leve e le condizioni organizzative per l'efficacia dell'eGovernment*, Soveria Mannelli, Rubbettino, 2007.
Quaranta M. (a cura di), *Il Codice della Pubblica Amministrazione Digitale*, Napoli, Liguori Editore, 2006.
Rabbito C., *L'informatica al servizio della Pubblica Amministrazione e del cittadino*, Gedit Edizioni, Bologna, 2007.
Riem G., *Sistema Pubblico di Connettività*, in Borruso R., Riem G., Sirotti Gaudenzi A., Vicenzotto P. (a cura di), *Glossario di diritto delle nuove tecnologie e dell'e-government*, Milano, A. Giuffré Editore, 2007.
Romano A., Marasso L., Marinazzo M., *Italia chiama eGovernment*, Milano, Guerini e Associati, 2008.
Sarcone V., *Per un'innovazione delle politiche governative: l'eGovernment*, articolo disponibile all'URL, consultato nel mese di ottobre 2009: http://www.diritto.it/materiali/tecnologie/sarcone.html.
Schumpeter J., *L'essenza e i principî dell'economia teorica*, Roma-Bari, Laterza, 1982.
Id. *Il ciclo economico*, Salerno, Palladio, 1979.
Cfr. Touraine A., *La società post-industriale*, Bologna, Il Mulino, 1970.
Ziccardi G., *Etica e Informatica*, Milano, Pearson Paravia Bruno Mondadori, 2009.
Zuccarini M., *Dieci anni di governo elettronico in Italia: destra e sinistra a confronto*, in "Polis", n. 1, 2007.

SITOGRAFIA

http://www.astrid-online.it/
http://www.ccegov.eu/
http://www.consiglio.regione.toscana.it/
http://www.cnipa.gov.it/
http://www.cortecostituzionale.it/
http://www.diritto.it/
http://www.european-eparticipation.eu/
http://www.europa.eu/
http://www.federalismi.it/
http://www.funzionepubblica.it/

Rivista elettronica di Diritto, Economia, Management

N. 1 - 2010 · pp. 162-180

L'amministrazione digitale. Progetti e tecnologie per l'e-government

Pasquale Luigi Di Viggiano

Abstract: L'Amministrazione pubblica digitale rappresenta un obiettivo il cui perseguimento è costellato da successi e da fallimenti che hanno consentito alle politiche di innovazione di avviare un processo rivoluzionario silenzioso e incruento che sta portando lentamente, ma inesorabilmente la PA verso la realizzazione di quell'idea conosciuta come governo elettronico: l'e-government. I fattori che lo compongono sono principalmente di natura culturale, organizzativa e tecnologica. L'applicazione delle norme che regolano la costruzione della PA digitale si scontra con una residua e tenace incapacità delle PA di scrollarsi di dosso la zavorra di un'organizzazione amministrativa con radici ottocententesche.
Le norme e le tecnologie preparano e presuppongono un processo di innovazione che esige innanzitutto un ripensamento dell'assetto organizzativo dell'amministrazione pubblica attraverso l'uso delle ICT, del Web, della dematerializzazione e degli strumenti giuridici e tecnologici che garantiscano sicurezza.

Although the achievement of electronic public administration and digitalization is a tormented process with ups and downs, innovation policies have been able to start up a revolutionary process, silently and steadily, that slowly but inevitably will lead to the realization of the so-called e-government.
Its components have mainly cultural, organizational and technological characteristics. The application of the rules that govern the establishment of digital public administration comes up against a residual and persistent incapacity of public administration to jettison the ballast of an administrative organization still rooted in the 19th century.
Regulations and technologies imply an innovation process that requires in the first place a rethinking of the organization of public administration by using ICT, the Web and dematerialization, as well as legal and technological tools that should guarantee security.

Parole chiave: E-government, Amministrazione digitale, Reingegnerizzazione, Firma digitale, Documento informatico, Sistemi esperti, Web, E-mail, Dematerializzazione.

Articolo pervenuto il 26 settembre 2010, approvato il 20 novembre 2010

1. Premessa

La società contemporanea viene definita come *società del rischio*[1], come *società globale*[2], come *società dell'informazione*[3]. In tutti i casi la comunicazione è il denominatore comune che da una parte connota positivamente la società contemporanea come comunicazione globale e dall'altra descrive i rischi e i pericoli che dall'esercizio comunicativo scaturiscono. Tuttavia, ciò che rende possibile parlare di *società globale dell'informazione* risiede nell'innovazione tecnologica che, con un'irruenza mai registrata nelle vicende umane pregresse, ha reso disponibili le *Information and Communication Technologies* (d'ora in avanti ICT) e ha velocemente trasformato i modelli di riferimento della società globale, partendo dalle organizzazioni formali[4]. Questo consente di rappresentare la transizione dal modello burocratico amministrativo, adottato a partire dalla struttura prussiana dell'organizzazione dello Stato, verso modelli più dinamici dell'amministrazione pubblica supportati e resi possibili proprio dalle ICT. La larga applicazione di queste tecnologie e la loro continua evoluzione verso un controllo organizzativo sempre più avanzato consentono di prefigurare orizzonti applicativi che rapidamente diventano obsoleti, rendendo arcaiche quelle intuizioni che la fantascienza più spinta collocava in un futuro lontano. Le tecnologie informatiche e le reti di computer, che attualmente rappresentano l'*hard core* delle conoscenze tecnologiche, anche di generazioni lontane dalla tecnologia più evoluta, avanzano così rapidamente da non consentire pause di assestamento che altre civiltà hanno conosciuto rispetto alle innovazioni tecnologiche ivi prodotte. Pensiamo alla stampa e alla sua diffusione.

---

[1] Il concetto di rischio assume particolare significato nelle riflessioni prodotte dalla sociologia contemporanea per descrivere in modo diverso gli esiti delle attività di selezione in base a scelte. In tutti i casi in cui tratteremo di rischio, intendiamo per *rischio* un possibile danno derivante da scelte soggettive, ma anche come unica possibilità che abbiamo per *costruire vincoli per il futuro*; con *pericolo* ci riferiremo alla possibilità che si verifichi un danno in seguito a scelte di altri. Cfr: R. De Giorgi, *Il rischio nella società contemporanea*, in R. De Giorgi, *Temi di filosofia del diritto*, Pensa Multimedia, Lecce 2006., pp. 55-68. Una letteratura che diventa sempre più ampia si occupa del rischio nella società, definendo addirittura la società contemporanea come "società del rischio". Cfr. N. Luhmann, *Sociologia del Rischio*, Bruno Mondadori, Milano 1996; A. Marinelli, *La costruzione del rischio,* Angeli, Milano 1993; M. Douglas, *Rischio e colpa*, Il Mulino, Bologna 1996; U. Beck , *Un mondo a rischio*, Einaudi, Torino 2003; Id., *La società del rischio,* Carocci, Roma 2006; Id., *I rischi della libertà,* Il mulino, Bologna 2000; A. Giddens, *Le conseguenze della Modernità*, Il Mulino, Bologna 1994.

[2] Cfr. U. Beck., *La società globale del rischio*, Asterios, Trieste 2001. Per una descrizione sintetica dei meccanismi che operano nell'economia mondiale e che definiscono "Globalizzazione", cfr. G. Lafay, *Capire la globalizzazione*, Il Mulino, Bologna, 1996. Interessate proposta di spiegazione della genesi (sociologica) della globalizzazione: … *poiché l'espansione e la velocità raggiunta dai media della diffusione rendono ormai possibile l'esperienza della simultaneità dell'accadere in tutte le regioni della terra e rendono possibile allo stesso tempo spiegare l'accadere attraverso la semplificatrice costruzione di catene causali, si è cominciato ad usare il termine globalizzazione.* R. de Giorgi*, Temi di filosofia del diritto,* cit., p. 17. Cfr. M. Castells, *Globalizzazione, identificazione e lo Stato: uno Stato senza poteri o uno stato a rete?,* in Id. , *Il potere delle identità*, Università Bocconi editore, Milano 2004

[3] Cfr. D. A. Limone, M. Mancarella, G. Preite (a cura di), *Turismatica: un nuovo paradigma della società dell'informazione*, Collana di Studi sulla Società dell'Informazione, Editrice UNI Service, Trento 2008; A. Mattelart, *Histoire de la societé de l'information*, (trad. it. di Sergio Arecco), *Storia della società dell'informazione*, Giulio Einaudi editore, Torino 2002. Interessante per una migliore comprensione della problematica, le argomentazioni avanzate in N. Negroponte, *Begin Digital*, , Vintage, New York 1995 (trad. it., *Essere digitali*, Sperling&Kupfer, Milano 1995).

[4] Per un approccio classico alle teorie dell'organizzazione da un punto di vista delle scienze sociali, cfr. A. Etzioni, *Sociologia dell'organizzazione*, Il Mulino, Bologna 1967.

Alcuni studiosi della società hanno individuato nelle tecnologie e nelle reti digitali gli elementi per proclamare l'avvento di nuove forme di democrazie[5] e, contemporaneamente, descrivono nuove forme di disuguaglianze e di esclusione[6].

L'impatto pubblico più diffuso che si registra in relazione alla disponibilità e all'uso delle tecnologie dell'informazione riguarda sicuramente lo sforzo istituzionale di realizzare l'Amministrazione Pubblica Digitale. In questa operazione epocale mondiale, occupa una posizione di rilevo la determinazione con cui l'UE[7], e anche l'Italia, perseguono la realizzazione di questo modello di società attraverso una produzione importante di norme innovative e il finanziamento di azioni tese a realizzare operativamente ciò che le norme indicano sul piano giuridico. Con l'ausilio delle ICT.

Parlare oggi di amministrazione digitale significa considerarne il quadro d'insieme ma, soprattutto, conoscere i singoli elementi che lo compongono. Significa principalmente osservare e descrivere i successi e i fallimenti che hanno consentito alle politiche di innovazione introdotte nella Pubblica amministrazione di avviare un processo rivoluzionario che non ha bisogno di sommosse popolari o di diffuse azioni cruente spargimenti di sangue, ma è una rivoluzione silenziosa che sta portando lentamente, ma inesorabilmente la PA verso la realizzazione di quell'idea conosciuta come governo elettronico: l'e-government. L'osservazione di questo processo, che è insieme sociale, politico, organizzativo e tecnologico, consente di descrivere i passaggi da uno stadio all'altro della sua evoluzione attraverso la descrizione dei settori che ne compongono la complessità.

Il sistema del diritto e le norme che disegnano gli aspetti giuridici e regolamentari dell'innovazione tecnologica della PA si sono dipanati sincronicamente al sistema economico di riferimento, facendo emergere lentamente la consapevolezza che un processo di innovazione tecnologica esige innanzitutto un ripensamento dell'assetto organizzativo dell'amministrazione pubblica.

Questo percorso,visto dalla prospettiva del diritto e della produzione di norme specifiche tese ad affermare un nuovo modello di amministrazione pubblica, può essere descritto con l'utilizzo di una metafora. La produzione di norme e la loro applicazione, sia a livello europeo che nazionale, ha seguito un andamento discontinuo e altalenante, presentando aspetti che

---

[5] Cfr. D. de Kerckhove, A. Tursi (a cura di), *Dopo la democrazia? Il potere e la sfera pubblica nell'epoca delle reti*. Apogeo,Milano, 2006, p. VIII. Vedi anche L. Gallino, *Tecnologia e democrazia*, Einaudi, Torino 2007.

[6] Cfr. A. Mattelart, *Histoire de la societé de l'information*, cit.. Il testo si pone in una posizione critica rispetto all'esaltazione delle tecnologie della comunicazione e avanza seri dubbi sulle capacità terapeutiche della comunicazione a distanza che attraverso le reti configurano nuovi modelli di potere e di egemonia culturale, quando non anche di nuove forme di sopraffazione. In questa ottica l'autore parla di *arcipelago delle differenze* all'interno del quale identifica una forma dell'esclusione che denomina *tecno-apartheid*. (pp. 132-143). L'era della comunicazione digitale e della telematica ha prodotto nuove uguaglianze (omologazioni) e altrettante nuove disuguaglianze che, in questo ambito, vengono definite generalmente come "digital divide". Lo studio del fenomeno descrive come questo produca nuove forme di disuguaglianze "digitali" nella *società dell'informazione* ma anche da un punto di vista lessicale produce espressioni per indicare inclusione digitale *(e-inclusion)* e analoga esclusione *(e-esclusion)*. Per una riflessione critica, cfr. S. Bentivegna, *Disuguaglianze digitali. Le nuove forme di esclusione nella società dell'informazione*, Laterza, Roma-Bari 2009.

[7] Per una conoscenza esaustiva delle attività normative, regolamentari e di indirizzo esercitate dalla UE in materia di Società dell'informazione, cfr. il sito web: http://europa.eu/legislation_summaries/information_society/index_it.htm.

richiamano le strategie di Penelope nel tessere e disfare la sua tela. Difatti, abbiamo assistito a iniziative legislative di grande portata innovativa e di notevole spessore di civiltà seguite subito dopo da scelte operative involute e anacronistiche che mal si conciliano con l'intento di innovare la P.A. Mentre da un lato il diritto nazionale produceva una norma epocale relativa alla validità giuridica del documento informatico attraverso l'uso di uno strumento assolutamente originale ed innovativo, oltre che sicuro: la firma digitale, dall'altra il diritto comunitario la intaccava solo pochi anni dopo introducendo varie tipologie di firme elettroniche che, in sostanza, rendevano e rendono meno cogente l'uso della firma digitale.

La mancanza totale di sanzioni, fino al 2009, relative all'applicazione delle norme per rendere la PA digitale, ha prodotto un paradosso preoccupante dal punto di vista del diritto: molte norme sono rimaste inapplicate, del tutto o in parte, mentre per spingere ad applicarne alcune il Legislatore ha dovuto emanare ulteriori norme che sono intervenute a normare quanto già il diritto imponeva. Questa difficoltà di attestarsi dell'amministrazione digitale si spiega con la portata assolutamente innovativa sia delle norme che delle ICT applicate alla PA il cui effetto da una parte ha suscitato pubblici entusiasmi e dall'altra ha impattato con una cultura datata e conservatrice di cui le risorse umane impiegate nella PA erano portatrici (dipendenti e dirigenti), determinando rifiuti e sospetti verso una materia che scardinava acquisizioni e pratiche lavorative (organizzative) ormai ampiamente consolidate. Anche se non più funzionali al contesto della società contemporanea e al nuovo modello di relazioni tra pubblica amministrazione e cittadini "utenti" che si sta affermando.

Osservare come questa tela si è costruita di giorno, con le costanti acquisizioni normative, e di come veniva disfatta di notte, con la loro altrettanto costante e pervicace disapplicazione, rappresenta il nodo sciogliendo il quale è possibile rappresentare le acquisizioni evolutive di una materia ancora *in fieri* culturalmente e organizzativamente, ma anche in fase di continuo superamento tecnologico e applicativo.

L'e-government rappresenta l'impegno, non solo nazionale, ma globale della società dell'informazione che si realizza attraverso la promozione di iniziative finalizzate a rendere disponibile e fruibile l'amministrazione digitale per cittadini e imprese. I segmenti e i progetti che danno corpo all'e-government segnano l'indice attraverso il quale è possibile misurarne lo sviluppo. *L'E-Government Development Index 2010* delle Nazioni Unite è lo strumento del Dipartimento degli affari sociali ed economici dell'ONU che dal 2003 pubblica un articolato studio annuale che analizza progetti, iniziative e stati avanzamento dei sistemi di governo elettronico avviati nei diversi paesi del mondo.

Il rapporto pubblicato nel 2010 analizza l'e-government in un periodo di crisi, economica e finanziaria, che investe buona parte del mondo occidentale. I dati emersi[8] hanno messo in

[8] I numeri, nella loro essenzialità, esprimono spesso molto più di quanto non possano fare le parole. Così la seconda parte del Rapporto propone *l'E-government Development Index*, una sintesi numerica di quanto analizzato dallo studio. Come tutti gli indici, anche l'*EGDI* non propone verità assolute ma scenari evolutivi; fotografa lo stato di fatto e suggerisce, nel confronto tra paesi, le tendenze in atto.
L'EGDI è il frutto di un punteggio complesso, assegnato alla volontà e alla capacità effettiva dimostrata sul campo dalle amministrazioni centrali di utilizzare la tecnologia online e mobile nella realizzazione delle proprie funzioni amministrative. Il panel esaminato è composto da 183 paesi. Articolato il set di indicatori misurati, studiati in modo che l'EGDI non catturi lo sviluppo dell'e-government in prospettiva assoluta ma, piuttosto, permetta di cogliere

luce un fenomeno in parte inatteso: nonostante la crisi, la richiesta di competenze specifiche e di progetti per il governo elettronico della PA è in crescita, insieme alla crescente richiesta di maggior trasparenza. Sembra, infatti che la crisi, a fronte di risorse sempre più scarse, costringa tutti al rigore e all'efficienza e l'introduzione dell'ICT trova in questo contesto più spazio di quanto si potesse intuire come strumento per ricostruire parte della fiducia persa dai cittadini verso pubblico. Questo trend è evidenziato nel Rapporto dai progressi registrati in molti paesi che in questi anni hanno scelto di non ridimensionare gli investimenti IT già previsti. Nei primi 20 Paesi più competitivi a livello mondiale non è presente l'Italia, collocata al 38esimo posto[9].

2. Gli elementi d'innovazione

L'amministrazione pubblica digitale trova la sua prima espressione in due fatti che singolarmente attengono a due sfere tra loro, sembrava, inconciliabili: la tecnologia informatica e la validità giuridica dei documenti amministrativi posta alla base di qualunque procedimento amministrativo legale.
Il progressivo perfezionamento tecnologico di word processor utilizzabili per la scrittura di testi digitali evoluti e la sempre maggiore disponibilità di applicazioni informatiche in grado di snellire la formazione e il trattamento del documento amministrativo ha consentito alle PA di orientarsi a produrre i propri documenti direttamente in formato digitale[10]. Tuttavia, al fine di renderli giuridicamente rilevanti la pratica più diffusa tendeva a trasformarli nuovamente in firmato analogico: cioè stamparli su un supporto materiale (carta in genere) e sottoscriverli, dotandoli, ove richiesto dalle norme, di timbri e punzoni.
L'introduzione nell'ordinamento giuridico italiano della validità del documento amministrativo elettronico formato secondo criteri previsti dalle norme e da standard tecnologici di sicurezza e a cui venivano associate firme elettroniche, ha costituito il punto di partenza ed ha posto le fondamenta di ciò che oggi definiamo come Amministrazione digitale.
In Italia, a partire dal DPR 445 del 2000, ad un atto volontario della PA di adottare strumenti tecnologici evoluti per l'esercizio delle attività amministrative, si aggiunge un obbligo circa i modelli tecnologici ed amministrativi da adottare nella gestione del flusso documentale amministrativo, introducendo la regolamentazione del protocollo informatico. Come sostenuto in altra occasione, allora, è la verifica del *contesto organizzativo* più idoneo

lo scostamento rispetto a quanto costruito dagli altri paesi. La scala utilizzata va da 0 a 1, espressione quest'ultimo del massimo livello possibile di sviluppo. Dal punto di vista matematico si tratta della media pesata di tre punteggi normalizzati relativi alle tre principali dimensioni del "governo elettronico": obiettivi e qualità dei servizi online, connettività, capitale umano. Ogni dimensione è a sua volta il frutto di un set di indicatori, il cui punteggio finale può essere analizzato autonomamente rispetto all'indice finale.

9 Cfr. *United Nations E-Government Survey 2010. Leveraging e-government at a time of financial and economic crisis*. http://www2.unpan.org/egovkb/global_reports/10report.htm.

10 A partire dal D. Lgs. 82/2005 e successive integrazioni, la PA ha l'obbligo di produrre i propri documenti *normalmente* in formato digitale e solo eccezionalmente, in formato analogico. Cfr. D. Lgs. 82/2005, art. 40 – Formazione di documenti informatici.

per i processi di innovazione tecnologica e di e-government l'operazione da compiere per analizzare le condizioni organizzative, piuttosto che quelle tecnologiche. Su queste basare, poi, la costruzione di pratiche innovative di amministrazione. Infatti, se il contesto organizzativo non risponde a "concreti" *parametri* di efficienza, efficacia, pubblicità ed economicità (nuovi modelli organizzativi; reingegnerizzazione dei processi e delle attività; controllo di gestione; contabilità analitica; protocollo informatico; servizi in rete; qualità dei servizi all'utenza; ecc.) anche lo stesso processo di e-government viene messo in discussione, anzi stenta a decollare. Di qui, la necessità di considerare il back-office (le strutture e le funzioni interne) come prerequisito per un front-office (siti, portali, sportelli, ecc.) istituzionale in grado di fornire informazioni validate, transazioni garantite e servizi *on line*. L'esperienza degli ultimi più recenti anni dimostra che intervenendo con sistematicità sul *back-office* certamente è possibile assicurare processi di automazione utili anche al *front-office*. Si riportano così i processi di innovazione tecnologica nell'ambito di quelli organizzativi supportati dai processi innovativi istituzionali [11].

Una delle discipline che più ha contribuito alla costruzione degli step attraverso i quali lentamente prende corpo quella che abbiamo definito *amministrazione digitale* è l'Informatica giuridica[12] che, confrontandosi con le tecnologie informatiche digitali, le traduce in ipotesi normative e in prassi concrete di operatività della P.A. Nel corso degli anni, proprio ricorrendo a questo fecondo rapporto, gli ambiti più innovativi che si occupavano di elaborazione automatica delle informazioni hanno ripreso alcuni temi che per la loro alta specificità avevano caratterizzato la ricerca di cibernetici e di informatici orientati all'automazione, trasponendone le acquisizioni più innovative nel campo del diritto e della Pubblica amministrazione in genere. Si comincia a parlare, così, anche in riferimento alle attività amministrative, di *Intelligenza Artificiale* (IA)[13], di *Sistemi esperti*[14] e, da ultimo, di *Business intelligence*[15].

L'esigenza di automatizzare operazioni amministrative e decisionali, via via sempre meno banali, ha condotto i ricercatori sociali ad occuparsi di materie sempre meno teoriche ed orientate alla soluzione di problemi che la crescente complessità delle attività amministrative producono. Si comincia, in questa maniera, a parlare sempre più spesso di *Intelligenza artificiale* come di quelle attività svolte tramite computer in grado di sostituire l'uomo. Infatti con il

---

[11] Cfr. P. L. Di Viggiano, *L'amministrazione digitale negli Enti Locali. I modelli organizzativi e gli strumenti tecnico-giuridi*ci, in M. Mancarella (a cura di), *Profili negoziali e organizzativi dell'amministrazione digitale*, Isegoria - Collana di Scienze Politiche, Giuridiche e dell'Amministrazione. Tangram Edizioni Scientifiche, Trento 2009, pp. 177-213.

[12] Giovanni Sartor ha sottolineato che "l'informatica giuridica è la disciplina che studia gli aspetti giuridici della rivoluzione tecnologica, economica e sociale prodotta dall'informatica; l'elaborazione automatica delle informazioni". Cfr. Sartor G., *Corso d'Informatica Giuridica*, Giappichelli, Torino 2008, p. IX. Il 1 dicembre 1995, promosso dall'ANDIG, si è tenuto a Roma il Convegno "L'informatica giuridica oggi" i cui atti, raccolti a cura di N. Palazzolo, rappresentano il manifesto della disciplina. Cfr. N. Palazzolo (a cura di), *L'informatica giuridica oggi. Atti del Convegno Andig* (Roma, 1° dicembre 2005), Collana ITTIG- CNR - Firenze, Edizioni Scientifiche Italiane, Napoli 2007.

[13] Cfr. S. J. Russell; P. Norvig, S. Gaburri (a cura di) *Intelligenza artificiale. Un approccio moderno (2)*, 2ª edizione, Pearson Education Italia, Milano 2005.

[14] Cfr. G. Iacono, *La creazione di un sistema esperto*, Franco Angeli, Milano 1991; D. W. Rolston, *Sistemi esperti: teoria e sviluppo*, McGraw-Hill libri Italia, Milano 1991.

[15] Cfr. L. Quagini, *Business intelligence e knowledge management. Gestione delle informazioni e delle performances nell'era digitale*. Franco Angeli, Milano 2004. Cfr. anche http://it.wikipedia.org/wiki/Business_intelligence.

termine *Intelligenza Artificiale*[16] (IA) si indicano le capacità di un computer di svolgere funzioni e "ragionamenti" propri della mente umana. Per la sua caratteristica di presentare aspetti teorici e pratici, lo studio dell'IA riguarda scienziati e umanisti, teorici del linguaggio, cibernetici, filosofi e giuristi.

Da un punto di vista tipicamente informatico essa si occupa di teorie e tecniche di sviluppo di algoritmi in grado di consentire ai calcolatori di mostrare abilità e attività "intelligenti", spesso relegate in domini specifici. La pubblica amministrazione è uno di questi domini specifici in cui la IA trova applicazione.

Durante i primi anni settanta del secolo scorso si assiste allo sviluppo dei *sistemi di produzione*, ossia di programmi che sfruttano un insieme di conoscenze organizzate in base di dati, attraverso l'applicazione di regole di produzione, per ottenere risposte a domande precise.

I *sistemi esperti* sostituiscono successivamente i sistemi di produzione per via delle difficoltà incontrate da questi ultimi, con particolare riferimento alla necessità di fornire inizialmente la conoscenza in forma esplicita e la poca flessibilità delle regole di produzione. Questi sistemi mostrano le enormi possibilità offerte da un efficace sfruttamento di (relativamente) poche basi di conoscenza per programmi capaci di prendere decisioni o fornire avvisi in aree diverse. In pratica l'analisi dei dati viene razionalizzata e generalizzata. A causa delle loro specifiche caratteristiche i sistemi esperti rappresentano per la PA l'applicazione della IA in un ambito ben preciso: l'amministrazione.

I sistemi esperti sono stati impiegati in varie aree dell'amministrazione pubblica, in particolare nel sistema giudiziario, nel sistema fiscale e dei tributi, nel sistema sanitario, e sono stati individuati come quello strumento in grado di far raggiungere all'amministrazione di riferimento, livelli elevati di automazione in tutte le fasi che compongono le attività amministrative, fino a sperimentare la possibilità di formulare automaticamente, o con pochi interventi umani, documenti complessi contenenti decisioni o provvedimenti finali di un procedimento amministrativo. Il presupposto tecnologico è rappresentato, in questo caso, da un sistema di dati raccolti e organizzati tramite data base (data warehouse) la cui completezza, ridondanza, attendibilità e integrità dovrebbe consentire risposte congruenti a quesiti anche complessi, orientando la risposta anche in base ad elementi in grado di contestualizzare il report (output). Sono i presupposti che riassumono le aspettative di Lee Loevinger partendo dai quali è nata l'attuale disciplina dell'Informatica giuridica[17] che, tuttavia, non può essere relegata solo alle problematiche connesse all'utilizzo dell'informatica ai vari ambiti ed aspetti del diritto. Oggi assistiamo ad iniziative più che proficue di applicazione degli esiti scientifici

---

[16] L'espressione "Intelligenza Artificiale" (Artificial Intelligence) fu coniata nel 1956 dal matematico americano John McCarthy, durante uno storico seminario interdisciplinare svoltosi nel New Hampshire. Secondo le parole di Marvin Minsky, uno dei pionieri della I.A., lo scopo di questa nuova disciplina sarebbe stato quello di *far fare alle macchine delle cose che richiederebbero l'intelligenza se fossero fatte dagli uomini*. Un punto di svolta della materia si ha con un famoso articolo di Alan Turing sulla rivista *Mind* nel 1950. Nell'articolo viene indicata la possibilità di creare un programma al fine di far comportare un computer in maniera intelligente. Quindi la progettazione di macchine intelligenti dipende fortemente dalle possibilità di rappresentazione simbolica del problema. Cfr. S. J. Russell; P. Norvig, S. Gaburri (a cura di), *Intelligenza artificiale. Un approccio moderno*, cit..

[17] Cfr. L. Loevinger, *Jurimetrics. The Next Step Forward*, Minnesota Law Review, 1949. Cfr. per una sintetica trattazione dei temi relativi all'informatica giuridica, A. Pizzo, *Informatica giuridica: un inventario di problemi*, in «Diritto&diritti – Elettronic Law Review», pubblicata all'indirizzo http://www.diritto.it/pdf/26360.pdf.

dell'informatica giuridica nello studio e nella pratica delle attività amministrative, tanto che è possibile annoverare nell'ambito disciplinare dell'Informatica giuridica anche l'Informatica della PA[18].

3. Aspetti tecnologici dell'organizzazione

Il trend delle informazioni digitali generate e trattate dalla PA (non ancora del tutto) digitale registra, dal 2006, una crescita pari quasi al 50% annuo, così che gli Enti interessati dovranno preoccuparsi di tutte le operazioni legate a questo andamento e garantire le caratteristiche per i dati pubblici previste dal D. Lgs. 82/2005 ss.mm. (affidabilità, sicurezza, privacy, conservazione, ecc.). La gestione delle informazioni digitali (*governance*) sarà, dunque, una delle maggiori attività dalla PA nell'intento di realizzare politiche e pratiche di e-government[19].
L'esigenza primaria di garantire un nuovo modello organizzativo e una nuova pratica dell'organizzazione della PA che abbia razionalizzato le sue attività si correla alla disponibilità di strumenti di gestione del dato digitale che garantiscano un elevato livello di complessità tecnologica in grado di rispondere alle richieste di trattamento dei dati digitali pubblici e istituzionali. Per soddisfare questa esigenza si utilizzano *Sistemi Informativi* (intranet) che compendiano tecniche e infrastrutture in grado di rispondere a queste funzioni, compresa la sicurezza. Alcuni esempi di soluzioni tecnologiche-organizzative sono rappresentati dai sistemi riconducibili alla famiglia dell'*Enterprise Content Management* (ECM), ovvero dell'insieme di strumenti che consentono la gestione della documentazione prodotta, ricevuta e conservata all'interno di un'organizzazione, indipendentemente dal suo formato, con funzioni atte a *creare o acquisire, gestire, proteggere, archiviare, conservare, eliminare (quando necessario), ricercare, personalizzare/ modificare, visualizzare/ stampare, trasmettere, distribuire, utilizzare e pubblicare i contenuti digitali non strutturati ed i documenti coinvolti nei processi di una organizzazione* anche pubblica. L'ECM consente di gestire, insieme a queste informazioni, anche quelle strutturate, cioè quelle alla base delle tradizionali applicazioni transazionali.
I sistemi di ECM sono, generalmente, un insieme di altri sistemi:

- **Sistemi per gestire il processo di creazione**, revisione, approvazione e pubblicazione dei contenuti sul Web (Web Content Management). In questo caso possiamo parlare anche di Content management system[20].

---

[18] In particolare dopo l'intervento di Donato Limone nel convegno: *L'informatica giuridica oggi*, tenutosi a Roma nel 2005. Cfr. N. Palazzolo (a cura di), *L'informatica giuridica oggi. Atti del Convegno Andig* (Roma, 1° dicembre 2005), cit..

[19] Gli studi dell'Università di Berkeley e di IDC ci dicono che la quantità di informazioni digitali generate annualmente al mondo sta letteralmente esplodendo – è il commento di Vincenzo Gambetta, direttore scientifico di OMAT – andando dai 12 Exabyte (miliardi di miliardi di caratteri) generati nel 1998, ai 95 del 2005, agli 800 del 2009 ai 1.200 previsti per il corrente anno fino ad arrivare ai circa 35.000 previsti per il 2020. È evidente che quello della conservazione dei dati sia un tema quanto mai attuale.
http://www.freeonline.org/cs/com/cs-110258/Come_conservare_i_dati_digitali_nei_prossimi_mille_anni.

[20] Un *content management system*, in acronimo *CMS*, che letteralmente significa "sistema di gestione dei contenuti", è uno strumento software installato su un server web studiato per facilitare la gestione dei contenuti di siti web, esonerando l'amministratore del sito da conoscenze tecniche di programmazione Web. Tecnicamente un CMS è un'applicazione

- **Sistemi per la gestione dei record**, ossia quelle informazioni che le organizzazioni intendono conservare. Questo sistema per è utilizzato per identificare, catalogare, archiviare, conservare, proteggere ed, eventualmente, distruggere dati. Il sistema deve garantire, nel tempo, l'accesso ai record assicurando che non siano stati alterati/distrutti e pertanto siano, in ogni momento, legalmente rilevanti. Questi sistemi sono sovente indicati anche come *Records Management.*
- **Sistemi per sviluppare**, automatizzare, gestire, controllare ed ottimizzare i processi, inclusi quelli che coinvolgono automazione e persone e sono indicati spesso come *Business Process Management.* Le tradizionali applicazioni di Workflow Management si differenziano dalle applicazioni di BPM in quanto sono principalmente associate ai processi di gestione di documenti.
- **Sistemi per gestire** il "Ciclo di Vita" di grandi raccolte di contenuti digitali, quali immagini fotografiche, grafici, loghi, documenti complessi o Rich Media – In genere, i Contenuti gestiti da questo sistema sono composti da più di un elemento (video, suoni o dati) e vengono comunemente indicati come *Digital Asset Management.*
- **Sistemi per la gestione dell'intero** "Ciclo di Vita" dei documenti non strutturati, indipendentemente dalla loro origine (interna, esterna) o struttura; sono l'evoluzione dei tradizionali Sistemi Immagine, COLD, di Document Repository, (*Enterprise Document Management*);
- **Sistemi per accedere** e per gestire i contenuti di differenti, eterogenei e numerosi repository, con il compito di "consolidare" le informazioni ivi contenute al fine di offrire una visione univoca dei contenuti critici per l'amministrazione. L'integrazione dei contenuti è un elemento fondamentale in un sistema di ECM. Se i dati sono omogenei (Data Base, ad esempio) si può pensare al consolidamento, in maniera definitiva, in un'unica struttura delle informazioni dalle differenti origini. Tuttavia, spesso, è necessaria una forma meno "rigida" d'integrazione che mantenga le strutture originali, ma consenta di accedere ed aggiornare contenuti digitali di differente origine, formato, struttura e posizione. In questo caso parliamo di *Data Federation* e il sistema che li gestisce viene indicato come *Enterprise Content Integration.*

Questo contesto tecnologico la cui descrizione, essenziale e non esaustiva, costituisce il substrato infrastrutturale per la realizzazione di un sistema informativo avanzato per la PA richiede che la gestione documentale, utilizzando le regole tecniche di cui all'Art. 71 del CAD, debba necessariamente comprendere sezioni tra loro interfacciate per la realizzazione di un sistema di gestione documentale il cui *front end* è rappresentato dal protocollo informatico e il *back end* dall'archiviazione ottica con le caratteristiche organizzative e legali previste dalle norme.

Questo sistema è costituito da alcuni elementi essenziali e presenta generalmente un schema di questo tipo:

lato server che si appoggia su un database preesistente per lo stoccaggio dei contenuti e suddivisa in due parti: la sezione di amministrazione (back end), che serve ad organizzare e supervisionare la produzione dei contenuti, e la sezione applicativa (front end), che l'utente web usa per fruire dei contenuti e delle applicazioni del sito.

1. **Sistema di acquisizione**: Nella fase di accesso al sistema, di fronte alla necessità di trattare dati su supporto analogico, è richiesta la disponibilità di HD e SW in grado di trasformare in dato digitale qualsiasi input di carattere analogico. In questo caso una dotazione minima è costituita da scanner, più o meno evoluti e specializzati, e da famiglie di software in grado di riconoscere i caratteri e trasformarli in bit, normalmente indicati dalle seguenti tipologie di SW:
   - ICR - Riconoscimento intelligente dei caratteri
   - OCR - Riconoscimento ottico dei caratteri
   - OMR - Riconoscimento ottico dei checkbox
   - Riconoscimento della scrittura manuale
   - Riconoscimento di Barcode
2. **Sistema di gestione**: Il componente di Gestione si occupa del controllo, dell'indicizzazione e della verifica dell'integrità delle informazioni acquisite. In questo caso parliamo di:
   - Business Process Management (BPM)
   - Document management (DM)
   - Records Management
   - Web Content Management
3. **Archiviazione e conservazione**: I componenti per l'archiviazione sono utilizzati per quelle informazioni che non devono essere più modificate e necessitano di essere salvate permanentemente. I dispositivi più comuni al salvataggio delle informazioni sono: Hard disk (a diversa tecnologia, anche di rete, come NAS), Nastri Magnetici o Dischi ottici.
4. **Distribuzione**: Le informazioni create, gestite, archiviate e conservate, possono essere distribuite attraverso diversi canali. I principali canali di distribuzione sono: internet ed intranet, e-mail e, in futuro, Web TV, tecnologie e applicazioni per il mobile computing, ecc.
5. **Funzioni e servizi nella PA**: All'interno di una organizzazione pubblica il SI deve necessariamente garantire alcune funzioni inderogabili per il funzionamento corretto dei una PA digitale. In particolare bisogna che siano garantiti ambiti entro cui si realizzino operazioni di intranet:
   - Collaborazione e comunicazione nella creazione dei contenuti
   - Gestione Documentale e Workflow
   - Knowledge Management & Portali
   - Paperless: ovvero dematerializzazione, archiviazione digitale e conservazione sostitutiva
   - Ricerca delle informazioni e dei documenti

Una delle funzioni strategiche più rilevanti è rappresentata dalla possibilità di ricerca delle informazioni e dal tipo di motore di ricerca implementato. La difficoltà di ricerca in una Intranet è causata da diversi fattori quali:

- complessità dell'ambiente tecnologico cui si appoggiano le informazioni in assenza di standard consolidati
- differenti sistemi di classificazione

- fonti eterogenee (database, file system, sistemi documentali, ...) e distribuite su sistemi diversi.
- funzione delle differenti tipologie di "contenitori" che accolgono le informazioni
- poche correlazioni e ridondanze tra i documenti

Per effettuare, dunque, ricerche efficaci in una Intranet bisogna disporre di tecnologie in grado di associare ai contenuti informazioni di contesto (metadati) significative - a fronte di un efficace sistema di classificazione dei documenti.

Il sistema di comunicazione di una moderna PA digitale è garantito da norme e da tecnologie che presuppongono, per la loro reale applicazione, di un contesto organizzativo innovato e razionalizzato delle strutture pubbliche. La comunicazione, sia interna che esterna, è il cuore di tutto il sistema innovativo della PA. E-government si declina, in altri termini, come la possibilità delle PA di comunicare il dato digitale, opportunamente trattato, sia al proprio interno che all'esterno, finalizzato al servizio dell'utenza.

Le norme sulla comunicazione pubblica[21] e gli strumenti giuridici e tecnologico-organizzativi[22] indirizzano verso una multicanalità di relazioni *on line* i cui elementi portanti sono costituiti dalla posta elettronica e dai portali della PA. Anche in questo caso la delocalizzazione dell'informazione e la sua vocazione a soddisfare *device* mobili in sicurezza, la metafora della rete come descrizione della società contemporanea della comunicazione e la tendenza della PA a diventare digitale, ci conducono ad occuparci, seppure brevemente di alcuni elementi strutturali di questa società dell'informazione.

---

[21] Cfr. la Legge 150/2000 - "Disciplina delle attività di informazione e comunicazione delle pubbliche amministrazioni". Questa norma può ad oggi rappresentare il caposaldo normativo della comunicazione pubblica. Con essa la comunicazione delle amministrazioni pubbliche diviene *obbligo* e ne vengono definiti strumenti e soggetti. Con questa normativa la Comunicazione, o meglio l'Informazione, viene definita come risorsa fondamentale, quindi legittimata, e con la previsione che essa sia elemento principale dell'attività di una Pubblica Amministrazione. L'articolo 1 è il manifesto dell'intero impianto legislativo. Il comma 1 è chiarissimo *"Le disposizioni della presente legge, in attuazione dei principi che regolano la trasparenza e l'efficacia dell'azione amministrativa, disciplinano le attività di informazione e di comunicazione delle amministrazioni pubbliche".*

[22] Confronta, per tutte, il D. Lgs. 82/2005 e ss.mm. che, per i suoi contenuti innovativi è denominato Codice dell'Amministrazione Digitale (CAD).

4. I media della comunicazione digitale pubblica

Riteniamo che, in ambito di Amministrazione pubblica, possano essere indicati sinteticamente almeno tre strumenti che la rendono possibile; che rendono possibile che, a partire dal documento informatico, lo stesso si trasformi in documento amministrativo elettronico e la sua utilizzazione legale sia posta alla base delle attività amministrative innovate.

La firma digitale rende il documento informatico giuridicamente rilevante, oltre che dotarlo di livelli di sicurezza elevati; l'intranet, di cui ci siamo occupati, rende possibile la comunicazione interna, mentre la posta elettronica (compresa la versione certificata – PEC) e i siti web della PA rappresentano lo strumento e l'ambiente tecnologico che consentono il flusso organizzato di elettroni, di bit, in grado di assicurare quella che chiamiamo comunicazione digitale.

Il CNIPA definisce la firma digitale come "uno dei cardini del processo di e-government"[23].

L'Italia è uno dei Paesi in cui si registra un maggior uso legale della firma digitale avendo, peraltro, per primo, attribuito piena validità giuridica ai documenti elettronici fin dal lontano 1997 (con il DPR 513/97) ed essendo quello con maggiore diffusione in Europa.

Il CAD definisce la firma digitale *come un particolare tipo di firma elettronica qualificata basata 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.*

La particolare delicatezza di questo strumento crittografico, la cui robustezza rappresenta il limite invalicabile per la sicurezza del dato amministrativo e l'essenza stessa del diritto che la garantisce, ha richiesto nel tempo interventi di natura tecnico-giuridica che hanno di volta in volta aggiornato alle acquisizioni tecnologiche della crittografia più evoluta le norme e le pratiche di applicazione.

Nel tempo si sono accresciuti i formati e le modalità di utilizzo della firma digitale fino all'emanazione, in data 28 luglio 2010, della *Determinazione Commissariale n. 69/2010* che modifica la Deliberazione CNIPA n. 45/2009. In precedenza, il 6 giugno 2009 (G.U. 129) era stato pubblicato il decreto con le nuove regole tecniche sulle firma digitale, firmato dal ministro Brunetta a fine marzo. Fra le novità di rilievo l'apertura ufficiale all'utilizzo della firma digitale centralizzata o "remota". Con la norma viene, infatti, definito:

- quali sono i dati necessari per la creazione di una firma digitale, ovvero "l'insieme dei codici personali e delle chiavi crittografiche private, utilizzate dal firmatario per creare una firma elettronica";
- che il titolare della firma "mantiene in modo esclusivo la conoscenza o la disponibilità di almeno uno dei dati per la creazione della firma".

La formulazione "almeno uno" indica che il possesso esclusivo dei codici personali per accedere alla chiave privata (ad esempio un token OTP con relativo PIN) è sufficiente per la creazione di firme digitali pienamente legali.

La Deliberazione n. 45 del 21 maggio 2009 del CNIPA, interveniva a stabilire nuove regole

[23] http://www.cnipa.gov.it/site/it-it/Attivit%C3%A0/Firma_digitale/

per il riconoscimento e la verifica del documento informatico. In particolare:

1. precisando standard e regole per la composizione di documenti informatici e per il loro riconoscimento e verifica relativo ai certificatori accreditati
2. indicando gli algoritmi per la generazione e verifica della firma digitale.
3. definendo il profilo dei certificati qualificati e le informazioni che in essi devono essere contenute.
4. definendo il profilo e le informazioni che devono essere contenute nei certificati elettronici di certificazione e di marcatura temporale.
5. definendo le regole per la validazione temporale, il formato e le informazioni che devono essere contenute nelle marche temporali utilizzate dai sistemi di validazione temporale dei documenti, così come definiti dalle regole tecniche.
6. definendo i formati e le modalità di accesso alle informazioni sulla revoca e sulla sospensione dei certificati.
7. definendo i formati delle buste crittografiche destinate a contenere gli oggetti sottoscritti con firma digitale.
8. definendo i requisiti delle applicazioni di apposizione e verifica della firma digitale sulla base delle regole tecniche.

La novità più rilevante di questa Deliberazione è contenuta nell'art. 3. che dispone nuove regole per gli algoritmi crittografici utilizzati (più robusti) di firme digitali. In particolare i comma 1) e 2):

1. I certificatori accreditati devono utilizzare l'algoritmo RSA (Rivest-Shamir-Adleman) con lunghezza delle chiavi non inferiore a 1024 bit; le chiavi di certificazione di cui all'articolo 4, comma 4, lettera b) delle regole tecniche devono avere una lunghezza non inferiore a 2048 bit.
2. A partire dall'anno successivo a quello dell'entrata in vigore della presente deliberazione, le firme elettroniche apposte utilizzando algoritmi di crittografia asimmetrica basati sulle curve ellittiche hanno valore di firma digitale ai sensi della normativa vigente.

Partendo da queste nuove acquisizioni normative si è già diffusa l'idea che la firma digitale tradizionale, ovvero quella apposta su un documento informatico tramite il proprio dispositivo elettronico di firma installato ed utilizzabile sul proprio personal computer, potrebbe essere già superata dalle nuove tecnologie. La possibilità di firmare un documento informatico in modalità Remota e con l'utilizzo associato della Biometria comincia a rappresentare la nuova frontiera applicativa per aziende e PA, nonché per i privati.

Se intendiamo la Biometria, oltre che con la formula classica ormai accettata[24], anche come quel settore della biologia che misura e studia statisticamente i dati rilevati sugli esseri viventi, per compararne classificazioni e leggi, è possibile utilizzare la biometria e applicarla alla medicina tradizionale (esame del sangue, misurazione della temperatura o della pressione fino all'esame del *D.N.A)* . abbinata con *l'utilizzo della Firma Digitale Remota,* basata sull'utilizzo di un dispositivo sicuro centralizzato (HSM) per la generazione e la conservazione delle chiavi di firma.

---

[24] Cfr. G. Preite, *Il riconoscimento biometrico. Sicurezza versus privacy*, UNI Service, Trento 2007.

Per HSM intendiamo "Hardware Security Module", cioè un dispositivo hardware che contiene le chiavi crittografiche o di firma paragonabile ad una mega Smart Card con caratteristiche di sicurezza, resistenza ed efficienza estremamente elevate. Infatti gli HSM sono utilizzati per la firma elettronica e/o digitale ma possono contenere sia chiavi simmetriche che chiavi asimmetriche (coppie di chiavi pubblico/private e relativi certificati X.509) e non importano (o esportano) mai tali chiavi ma le generano o distruggono direttamente al loro interno. Quindi siamo in presenza di un dispositivo di massima sicurezza nella gestione dell'apposizione e verifica della firma digitale.

Possibile applicazione di questo sistema può essere un software di conservazione sostitutiva che permetta all'utente di utilizzare la firma digitale in modalità remota e impiegare questa metodologia anche per il login dell'utente al sistema di conservazione digitale, salvaguardando così i requisiti previsti dalla legge 196/2003 in materia di trattamento dei dati personali e di Privacy.

L'uso della Biometria potrebbe contribuire alle applicazioni di hardware e software di conservazione sostitutiva per la firma digitale in remoto di documenti informatici, eliminando la necessità del PIN di accesso. Il riconoscimento biometrico certo dell'utente che sta utilizzando il software consentirebbe alcuni fattori di riconoscimento: ritmo, velocità, pressione, accelerazione e movimento. All'atto di apporre una firma digitale a un documento informatico, saremmo di fronte ad un evento più sicuro nella generazione della firma, rispetto alla semplice digitazione del PIN.

In questa sede meritano un cenno anche le **e-mail**. Sia in ambito pubblico che privato l'uso della posta elettronica si è attestato come la quasi normalità di comunicazione non solo personale, ma anche orientata al business e all'esercizio delle funzioni della PA.

La comunicazione digitale e la dematerializzazione della PA sono sempre più caratterizzate dalla diffusione come prassi ordinaria e dalla gestione delle e-mail. L'art. 47 del CAD descrive come la PA debba fare uso della posta elettronica per la trasmissione di documenti tra le pubbliche amministrazioni che, di norma, comunicano tra di loro mediante l'utilizzo di e-mail poiché queste sono valide ai fini del procedimento amministrativo quando è possibile verificarne la provenienza. La firma digitale o il n. di protocollo informatico rappresentano alcuni dei requisiti insieme alla PEC, per certificare la loro validità. La Posta elettronica certificata (PEC) rappresenta il livello più elevato della comunicazione istituzionale con valore legale il cui uso è ampiamente previsto dal CAD (Artt. 6, 48).

Buona parte della comunicazione istituzionale delle PA "fluisce" attraverso le E-mail ed esse *contengono una quantità ingente di informazioni suscettibili di tutela legale*. Spesso la posta elettronica non è gestita in maniera strutturalmente organizzata e la sua utilizzazione (creazione, invio e conservazione) in ambito pubblico spesso è demandata alla sola buona volontà del dipendente, senza utilizzare applicazioni condivise preposte a ciò.

Per gestire le E-mail, attualmente, si hanno a disposizione due categorie di applicazioni, utilizzabili non solo in ambito business:

- la *E-mail Archiving* che affronta sostanzialmente il problema della capacità di archiviazione e mette a disposizione semplici strumenti per la loro conservazione e cancellazione. L'ottica di questo applicativo è quella di superare i limiti di capienza delle *Mail Box* personali e di agevolare e renderne più efficaci i backup.

- più sofisticate tecnologie che l'infrastruttura della gestione dei contenuti digitali ci mette a disposizione, se si vuole disporre delle informazioni che esse contengono, sono le *Enterprise Search* e i *Content integration*.

Il caso delle e-mail nella PA è un esempio del momento di riorganizzazione tardiva in atto e delle culture con cui si concepiscono le modalità con cui dati, informazioni e documenti sono generati, trasmessi e conservati. Nello stesso tempo il modo in cui non sono gestite è indicativo della resistenza al cambiamento che inevitabilmente accompagna ogni transizione. Queste informazioni, tuttavia, non rappresentano solo un "problema". L'informazione digitalizzata aumenta la capacità di comunicare, di condividere le informazioni e di fruire dei loro contenuti e può essere elaborata a tutto vantaggio dell'economia e della velocità dei Processi Produttivi, Amministrativi e di Business (efficienza, dunque) consentendo di rendere più veloce ed automatico tutto ciò che non richiede intervento umano. Si genera così un nuovo potenziale che contribuisce alla creazione di nuovi prodotti e alla fornitura di nuovi servizi (in poche parole, non solo efficienza, ma anche efficacia).

L'altro aspetto rilevante della posta elettronica è costituito dal fatto che il digitale "stravolge" il modo tradizionale di considerare le informazioni, ma anche l'approccio alla gestione e alla loro conservazione. L'informazione in formato digitale (documento informatico e sua sottoscrizione compresi) è lontana, non solo nella forma, ma anche nell'essenza da ciò a cui eravamo tradizionalmente abituati ed avevamo consolidato in norme e comportamenti, anche se è possibile prendere atto che la cultura del digitale si sta diffondendo in modo sempre più convinto anche tra coloro che hanno il compito di applicare norme, regolamenti, linee d'indirizzo e guide di comportamento: anche nella PA.

Il **Web** assume una rilevanza particolare e un posto di rilievo all'interno delle politiche di attuazione del modello di amministrazione digitale. A partire dal 6 agosto 1991, quando il fisico inglese Tim Berners-Lee pubblicò sul gruppo di discussione alt.hypertext i dettagli sul progetto WWW (World Wide Web) che "mirava a consentire la creazione di link a qualsiasi informazioni ovunque" si è sviluppata una cultura ed una tecnologia che ha condizionato tutte le reti di computer segnando progressi impensabili solo 20 anni fa. Per realizzare questo modello era stato sfruttato il sistema esistente dei cosiddetti ipertesti, usati per costruire una rete variamente incrociata di informazioni, organizzate secondo diversi criteri in modo da creare vari percorsi di lettura. Berners-Lee rese disponibile a tutti anche il software necessario per poter replicare ed *usare* la sua invenzione. Oggi utilizziamo reti connotate come Web 2.0 ed è in cantiere la realizzazione di reti di ultima generazione denominate Web 3.0[25].

---

[25] Cosa s'intende con Web 3.0. Può significare un'evoluzione della Rete che passi da uno strettissimo legame con i social network ovvero dall'interazione quotidiana e costante con milioni di milioni di internauti. La parola centrale diventa comunità (virtuale), la quale si alimenta di informazioni, amicizie, di soddisfazione dei propri bisogni (economici, sociali, ludici) attraverso la Rete. Diventa così decisivo il fattore tempo: il rapporto deve consumarsi "real time", in diretta. L'asse portante attorno a cui si organizzano le giornate e su cui confluiscono i pensieri si sposta sulla Rete. Facebook, Zynga e Amazon sono fra i primi a crederci con insistenza, investendo risorse economiche consistenti. Ma Web 3.0 è anche la digitalizzazione degli oggetti che abbiamo in casa. A dare una definizione del Web 3.0 con riferimento al contesto semantico, ci ha pensato Tim Berners-Lee, l'inventore del World Wide Web. "Le persone – ha recentemente affermato – si continuano a chiedere cos'è il Web 3.0. Penso che, forse, quando si sarà ottenuta una sovrapposizione della Grafica Vettoriale Scalabile, nel Web 2.0, e l'accesso a un Web semantico integrato attraverso un grosso quantitativo di dati, si potrà ottenere l'accesso a un'incredibile risorsa di dati". Cfr. Fabio Lepre, http://

Per la Pubblica amministrazione e per la realizzazione dell'e-government, il sito web, partendo da posizioni arretrate e marginali, è diventato lo strumento complesso in grado di realizzare un nuovo tipo di amministrazione pubblica e di fare evolvere lo stesso concetto di PA digitale. Le recenti *Linee guida per i siti web delle PA*, emanate a conclusione della fase di consultazione pubblica *on line* della loro versione preliminare del marzo 2010, erano state previste dalla Direttiva del 26 novembre 2009 n. 8 e sono rivolte a tutte le amministrazioni pubbliche, per le quali intendono avviare un processo verso il "miglioramento continuo" della qualità dei siti web pubblici[26].

Le Linee richiamano i concetti di accessibilità e usabilità già posti dalla Legge Stanca del 2004 (Legge 4/2004) e i contenuti minimi per i siti web della PA previsti nell'art. 54 del D. Lgs 82/2005, ma il loro valore aggiunto è riscontrabile nell'intento di porre ordine alle pubblicazioni web della PA che ha la necessità di passare dai "siti vetrina" ai "siti istituzionali". I primi, sorti dalla buona volontà di dipendenti "smanettoni" e spesso digiuni di ogni più elementare nozione teorica e pratica necessaria a costruire e pubblicare un sito web degno di questo nome, presentava no poche informazioni, scombinate e spesso non aggiornate, frutto di decisioni personali e non istituzionali, capaci di disorientare anche il più smaliziato degli internauti, la cui struttura impediva e impedisce ancora l'erogazione di qualsisasi servizio in rete, anche il più elementare.

I secondi rappresentano l'Istituzione e, utilizzando il dominio .gov.it, fugano ogni dubbio sulla natura istituzionale e pubblica del sito. La costruzione e la pubblicazione di questi siti web della PA sottostanno a norme precise, sebbene la loro violazione ad oggi non ha comportato sanzioni. La pubblicazione nella home page di almeno un indirizzo di PEC e l'utilizzo di caselle di posta elettronica istituzionale, si accompagnano alla pubblicazione degli organigrammi degli uffici, dei ruoli e dei recapiti istituzionali del personale delle PA. La realizzazione di questo modello e l'applicazione delle relative norme, sia detto per inciso, richiedono prima una completa reingegnerizzazione delle attività amministrative dell'Ente. Diversamente è un bluff, un adempimento formale incapace di rendere veramente digitale la PA.

Da un punto di vista della comunicazione e della gestione delle informazioni, le Linee Guida intervengono a individuare i profili professionali (ruoli) che devono gestire l'informazione pubblicata sui siti Web pubblici, stabilendo le funzioni e i criteri più corretti anche in relazione all'obbligo della pubblicazione degli atti nell'Albo pretorio on line.

Nell'*Appendice A4* delle Linee Guida, vengono, infatti, individuati i *Ruoli coinvolti nello sviluppo e nella gestione dei siti web della PA*. Ad alcuni ruoli "tradizionali" previsti della L. 150/2000, se ne affiancano di nuovi e importanti che operano nelle individuate due aree professionali di riferimento:

1. quella legato alle *competenze tecnologiche nell'ICT*, per la quale si individuano i ruoli di responsabile dei sistemi informativi, responsabile della sicurezza informatica, responsabile della gestione della rete, responsabile dell'accessibilità informatica, webmaster;

www.webmasterpoint.org/news/web-30-che-cose_p37380.html.

[26] http://www.innovazionepa.gov.it/comunicazione/notizie/2010/marzo/09032010---pubblicate-le-linee-guida-per-i-siti-web-delle-pa.aspx.

2. quello legata alle *competenze editoriali*, per la quale si individuano i ruoli di responsabile del procedimento di pubblicazione dei contenuti, Capo ufficio stampa, responsabile dell'ufficio relazioni con il pubblico, redattore web, web designer.

I riferimenti normativi, organizzativi e tecnologici sono disponibili. Lo sforzo dei prossimi anni sarà quello di applicarli nella direzione della costruzione della PA digitale.

6. Conclusioni

Questo breve excursus che ha inteso presentare alcuni elementi critici, descrittivi di una pubblica amministrazione che va lentamente modificandosi e degli strumenti giuridici, amministrativi e tecnologici che concorrono a rendere possibile il cambiamento, è necessariamente incompleto. Nondimeno l'interesse a osservare come la società contemporanea costruisce la propria modernità rappresenta lo stimolo a cercare gli elementi meno ovvii, ad individuare quelle latenze che sempre aspettano di emergere, quei paradossi all'interno dei quali si esplicitano le aporie che connotano ciò che di moderno caratterizza la PA.

A partire da questi presupposti abbiamo reso evidente come il modello burocratico dell'amministrazione pubblica italiana ha imboccato un percorso che porta ad obiettivi di non facile realizzazione e che, tuttavia, sarà necessario realizzare perché il salto epocale abbia luogo. La nuova era, a partire dagli anni '90 del secolo scorso con la legge 241/1990, è iniziata. Ciò che è esterno alla pubblica amministrazione ha una marcia che è dettata dal business e dagli interessi commerciali in una società rischiosa, ma globale. La sfida per la PA è necessariamente quella di rischiare per costruire il proprio futuro attraverso le scelte che lo renderanno possibile. Non ha alternative.

BIBLIOGRAFIA

- Beck U., *I rischi della libertà,* Il mulino, Bologna 2000
- Beck U., *La società del rischio,* Carocci, Roma 2006
- Beck U., *La società globale del rischio*, Asterios, Trieste 2001
- Beck U., *Un mondo a rischio*, Einaudi, Torino 2003
- Bentivegna S., *Disuguaglianze digitali. Le nuove forme di esclusione nella società dell'informazione*, Laterza, Roma-Bari 2009
- Castells M., *Il potere delle identità*, Università Bocconi editore, Milano 2004
- De Giorgi R., *Temi di filosofia del diritto*, Pensa Multimedia, Lecce, 2006
- Di Viggiano P. L., *L'amministrazione digitale negli Enti Locali. I modelli organizzativi e gli strumenti tecnico-giuridici*, in M. Mancarella (a cura di), *Profili negoziali e organizzativi dell'amministrazione digitale*, Isegoria - Tangram Edizioni Scientifiche, Trento 2009
- Douglas M., *Rischio e colpa*, Il Mulino, Bologna 1996;
- Etzioni A., *Sociologia dell'organizzazione*, Il Mulino, Bologna 1967
- Gallino L., *Tecnologia e democrazia*, Einaudi, Torino 2007

- Giddens A., *Le conseguenze della Modernità*, Il Mulino, Bologna 1994
- Iacono G., *La creazione di un sistema esperto*, Franco Angeli, Milano 1991
- Kerckhove D. de, Tursi A. (a cura di), *Dopo la democrazia? Il potere e la sfera pubblica nell'epoca delle reti*. Apogeo, Milano 2006
- Lafay G., *Capire la globalizzazione*, Il Mulino, Bologna, 1996
- Limone D. A., Mancarella M., Preite G. (a cura di), *Turismatica: un nuovo paradigma della società dell'informazione*, UNI Service, Trento 2008
- Loevinger L., *Jurimetrics. The Next Step Forward*, Minnesota Law Review, 1949
- Luhmann N., *Sociologia del Rischio*, Bruno Mondadori, Milano 1996
- Marinelli A., *La costruzione del rischio,* Angeli, Milano 1993
- Mattelart A., *Histoire de la societé de l'information*, (trad. it. di Sergio Arecco), *Storia della società dell'informazione*, Giulio Einaudi editore, Torino 2002
- Negroponte N., *Begin Digital*, , Vintage, New York 1995 (trad. it., *Essere digitali*, Sperling&Kupfer, Milano 1995)
- Palazzolo N. (a cura di), *L'informatica giuridica oggi. Atti del Convegno Andig* (Roma, 1° dicembre 2005), Collana ITTIG- CNR - Firenze, Edizioni Scientifiche Italiane, Napoli 2007
- Pizzo A., *Informatica giuridica: un inventario di problemi*, in «Diritto&diritti – Elettronic Law Review», pubblicata all'indirizzo http://www.diritto.it/pdf/26360.pdf
- Preite G., *Il riconoscimento biometrico. Sicurezza versus privacy*, UNI Service, Trento 2007
- Quagini L., *Business intelligence e knowledge management. Gestione delle informazioni e delle performances nell'era digitale*, Franco Angeli, Milano 2004
- Rolston D. W., *Sistemi esperti: teoria e sviluppo*, McGraw-Hill libri Italia, Milano 1991
- Russell S. J., Norvig P., Gaburri S. (a cura di) *Intelligenza artificiale. Un approccio moderno (2)*, 2ª edizione, Pearson Education Italia, Milano 2005
- Sartor G., *Corso d'Informatica Giuridica*, Giappichelli, Torino 2008
- *United Nations E-Government Survey 2010. Leveraging e-government at a time of financial and economic crisis*. http://www2.unpan.org/egovkb/global_reports/10report.htm

SITI WEB

http://europa.eu/legislation_summaries/information_society/index_it.htm

http://it.wikipedia.org

http://www.cnipa.gov.it

http://www.freeonline.org

http://www.innovazionepa.gov.it

http://www.webmasterpoint.org

http://www.italia.gov.it

NORME

- DPR 513/1997: Regolamento per attuazione firma elettronica (art.15 Decreto del Presidente della Repubblica 10 novembre 1997, n. 513) Regolamento recante criteri e modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici, a norma dell'articolo 15, comma 2, della legge 15 marzo 1997, n. 59
- Decreto Legislativo 7 marzo 2005, n. 82 - Codice dell'amministrazione digitale. (G.U.16 maggio 2005, n. 112 - S. O. n. 93) http://www.cnipa.gov.it/site/_files/CAD_01.pdf
- Legge 7 giugno 2000, n. 150 – "Disciplina delle attività di informazione e di comunicazione delle pubbliche amministrazioni" pubblicata nella *Gazzetta Ufficiale* n. 136 del 13 giugno 2000 - www.parlamento.it/parlam/leggi/00150l.htm
- Linee guida per i siti web della PA - art. 4 della Direttiva 8/09 del Ministro per la pubblica amministrazione e l'innovazione - ANNO 2010 http://www.innovazionepa.gov.it/media/571050/lg_sitiwebpa__26%20luglio%20 2010.pdf

Rivista elettronica di Diritto, Economia, Management

N. 1 - 2010 · pp. 181-191

ICT e innovazione:

la sfida del cambiamento organizzativo

Giulio Maggiore

Abstract: Le innovazioni tecnologiche connesse all'avvento della società dell'informazione hanno determinato una sostanziale modifica nel funzionamento delle organizzazioni pubbliche e private e negli equilibri competitivi di tutti i settori. Non tutte le imprese, però, hanno saputo cogliere le opportunità offerte dalle tecnologie ICT che pure negli ultimi anni sono diventate relativamente accessibili: ciò non è dipeso generalmente dalla mancanza di attenzione al problema, ma dalla difficoltà nel gestire il processo di cambiamento organizzativo. L'articolo analizza le ragioni profonde di queste difficoltà, che rivelano i limiti nello sviluppo di dynamic capabilities e rischiano di compromettere la competitività delle imprese nel medio periodo. Il cuore del problema viene identificato nell'aspettativa errata che gli artefatti tecnologici possa produrre il cambiamento: in realtà, ciò generalmente non accade, in quanto la tecnologia si trova ad interagire in un complesso sistema socio-materiale, dove il ruolo centrale è svolto dalle routine organizzative, da intendersi non come regole fisse di completamento, ma come "sistemi generativi che possono produrre un'ampia varietà di risultati in relazione alle circostanze". Se si vuole davvero gestire efficacemente il processo di innovazione, occorre rinunciare ad ogni illusione di determinismo tecnologico e intervenire sugli elementi umani e materiali che interagiscono nell'organizzazione orientando le dinamiche del sistema verso gli obiettivi strategici dell'impresa.

Technological innovations related to ICT have produced important changes in public and private organizations altering the competitive relationships within many different industries. Nevertheless, some organizations haven't been able to exploit the opportunity, even though the access to ICT in now very easy and relatively affordable. This failure doesn't generally depend on a lack of attention to the problem, but on the difficulty to manage organizational change. The paper explores the deep reasons why organizations don't succeed in achieving their innovation aims: a very serious failure, as it reveals the lack of dynamic capabilities, which could have a very negative impact on global competitiveness. The key explanation can be ascribed to the wrong expectation that technological artifacts can induce change, while usually this doesn't happen as technology is only one of the many factors interacting within a socio-material system where the main role is played by organizational routines. These cannot be conceived as formal and inflexible behavioral rules, but as "generative systems that can

Articolo pervenuto il 28 ottobre 2010, approvato il 3 dicembre 2010

produce a wide variety of performances". Therefore, in order to successfully manage innovation processes, organizations should abandon the idea of technological determinism and try to invest on human and material components, to modify routines and steer them towards the achievement of strategic goals.

Parole chiave: ICT, innovazione, dynamic capabilities, routine, information technology, gestione del cambiamento

Sommario: 1.L'impatto della società dell'informazione sulle organizzazioni - 2.Il ruolo delle dynamic capabilities - 3.Il rapporto complesso fra tecnologia e organizzazione - 4.Il cuore del problema: le routine organizzative - 5.Conclusioni: intervenire sulle routine per gestire il cambiamento

1. L'impatto della società dell'informazione sulle organizzazioni

L'avvento della società dell'informazione ha radicalmente cambiato il mondo delle organizzazioni, sia private che pubbliche, modificandone a volte in maniera radicale i processi strategici e operativi, fino al punto di sovvertire equilibri competitivi consolidati da tempo. Naturalmente ciò si è verificato in misura diversa in relazione ai differenti ambiti di azione.
In alcuni casi, l'impatto è stato tale da rivoluzionare la filiera stessa, aprendo spazi per nuovi competitor e mandando in crisi modelli di business fino a quel momento considerati molto solidi: si pensi, ad esempio, al settore della produzione e distribuzione musicale, dove il prodotto stesso ha cambiato forma, digitalizzandosi, così da risultare fruibile in modo diverso (lettori MP3) e da essere coinvolto in processi di vera e propria logistica virtuale, con degenerazioni difficilmente controllabili, come il fenomeno del peer-to-peer.
In altri settori più tradizionali, le tecnologie ICT hanno avuto un impatto meno evidente, in quanto non sono arrivate a toccare la natura stessa del prodotto e non sono state utilizzate massicciamente nei processi "core" delle aziende. Anche in questi casi, però, il ruolo delle nuove tecnologie è stato spesso più sensibile di quanto persino molti operatori del settore non abbiano percepito, in quanto ha trovato applicazione in segmenti meno visibili della *supply chain*, noti solo ad alcuni attori della filiera. Così, accade che quando un consumatore acquista un capo di abbigliamento dalla catena Zara, nemmeno immagina quanto la varietà e la velocità di assortimento di quel negozio dipendano dall'eccellenza dei sistemi informativi sviluppati a supporto della logistica del gruppo.
In realtà, l'elevato impatto dell'ICT sulla competitività delle imprese dipende dal fatto che – a prescindere dall'ambito specifico di attività – tutte le organizzazioni trattano una "materia prima" comune che entra in gioco in tutte le fasi della loro vita aziendale e in tutti i processi, da quelli strategici a quelli più banali: l'informazione. Un'informazione che entra nell'organizzazione attraverso un'attività costante di osservazione, raccolta dati, analisi; viene trattata, elaborata, trasformata; ritorna verso l'ambiente attraverso i molti canali di comunicazione

disponibili, ma anche attraverso i prodotti stessi, che incorporano e veicolano informazioni, oltre che utilità funzionali. Soprattutto in quella che sempre più spesso viene riconosciuta come economia della conoscenza, l'informazione è, quindi, la fonte primaria della creazione di valore, su cui si misura l'efficacia delle organizzazioni moderne (Rullani, 2004, 2006). In tal senso, le aziende possono essere viste come sistemi cognitivi fondati su *risorse di competenza* (ciò che l'impresa sa fare) e *risorse di fiducia* (come l'impresa viene percepita dai suoi interlocutori) che si combinano per produrre nuove risorse, alimentando così processi virtuosi di sviluppo (Vicari, 1991).

Le considerazioni proposte valgono anche e a maggior ragione nella Pubblica Amministrazione, dove la produzione si concentra su servizi ad altro contenuto informativo, che possono trarre grandi benefici da un'efficace applicazione dell'*information technology*, migliorando la qualità dell'offerta, contenendo i costi di erogazione e aprendo nuove opportunità di servizio in ambiti nemmeno ipotizzabili fino a qualche anno fa.

Non sorprende, pertanto, che tutte le organizzazioni abbiano guardato con grande interesse alle tecnologie dell'ICT, nella convinzione che queste potessero diventare la chiave per avviare processi di innovazione, tanto nel settore privato, dove sono progressivamente aumentati i budget destinati agli investimenti in tecnologie dell'informazione, quanto nel settore pubblico, dove i governi si sono lanciati, sia pure con tempi ed intensità diversificate, in ambiziosi programmi di e-government. In realtà, nonostante gli obiettivi e le logiche di fondo fossero condivise, i risultati sono stati molto diversi e non sempre direttamente proporzionali all'entità degli investimenti. In molti casi, infatti, né la determinazione del management né l'importanza delle risorse messe in campo hanno giovato più di tanto, portando a risultati decisamente inferiori alle aspettative, mentre in altri piccoli progetti d'investimento hanno prodotto risultati molto più profondi e duraturi, consentendo davvero quel salto di qualità che era nelle intenzioni dei promotori.

Da cosa dipende questa differenza? In una fase in cui le tecnologie informatiche sono diventate una vera e propria *commodity*, disponibile sul mercato con investimenti neppure eccessivi, cosa consente ad organizzazioni di sfruttarle per guadagnare un solido vantaggio competitivo, mentre altre non riescono a valorizzare le teoriche potenzialità degli strumenti tecnologici adottati? L'associazione fra nuove tecnologie dell'informazione e innovazione è spesso data per scontata, ma il passaggio è spesso molto complesso perché entrano in gioco dimensioni strategiche ed organizzative di elevata complessità, la cui scarsa considerazione può portare al fallimento di investimenti anche ingenti.

2. Il ruolo delle dynamic capabilities

La risposta al quesito sulla gestione efficace di processi di innovazione basati sulle nuove tecnologie ICT deve essere inquadrata in un più generale contesto di rivisitazione del concetto di "strategia", in atto da anni fra gli studiosi della materia, che tendono sempre di più a relativizzare la prospettiva dell'intenzionalità manageriale e della pianificazione formale, per adottare approcci di analisi più concentrati sulle dotazione di risorse e di competenze distintive (Wernerfelt, 1984; Barney, 1991; Rumelt, 1991; Grant, 1991; Peteraf, 1993). In quest'ottica - tipica

del paradigma che ha preso il nome di di *resource based view* - il valore della strategia non risiede tanto nella capacità di prevedere il futuro, disegnando scenari evolutivi per posizionare in maniera vincente l'offerta dell'azienda in uno spazio d'azione illimitato, ma nel patrimonio di risorse che si è in grado di costruire nel tempo per mettere l'organizzazione nella condizione ideale per fronteggiare le sfide competitive.

Il futuro non è più visto come un campo aperto in cui muoversi con piena libertà di scelta e di azione, ma come uno spazio complesso, difficilmente prevedibile e assolutamente non controllabile, dove le imprese possono mettere in gioco le loro *core competences* (Prahalad, Hamel, 1990) e le loro risorse (per lo più intangibili) in un confronto competitivo dinamico, dove i rapporti di forza si modificano continuamente (D'Aveni, 1995). Il futuro dipende dal passato secondo logiche di *path dependance*, che determinano la competitività di oggi sulla base di percorsi di accumulo delle risorse profondamente radicati nella storia delle organizzazioni. La visione prende il posto del piano e non capita di rado che le strategie dichiarate dalle imprese non siano altro che razionalizzazioni a posteriori di scelte fortemente vincolate dalle condizioni ambientali e organizzative che l'impresa si trova a dovere fronteggiare (Mintzberg, Waters, 1982; Mintzberg, 1994).

In questo scenario l'elemento determinate per la sopravvivenza e la crescita delle organizzazioni diventa, quindi, la possibilità di sviluppare, mantenere ed alimentare un patrimonio di "dynamic capabilities", ovvero una capacità di adeguare costantemente le proprie risorse critiche, producendo innovazione continua (Teece, Pisano, 1994; Teece, Pisano, Shuen, 1997; Winter, 2003; Helfat et al., 2007). In particolare, emergono quelle imprese che si dimostrano più capaci di altre nel riconoscere le migliori opportunità tecnologiche e di mercato (*sensing*), nel trasformare tali opportunità in processi, prodotti, servizi di successo (*seizing*), nel gestire il cambiamento organizzativo attraverso una riconfigurazione delle risorse e delle competenze disponibili (*managing*) (Teece, 2007).

Questo approccio consente di comprendere le ragioni per cui l'adozione di soluzioni basate sulle tecnologie ICT non sempre produce le performance attese. Il risultato dipende, infatti, non tanto dalle caratteristiche intrinseche delle tecnologie adottate quanto dalla capacità delle imprese di leggere correttamente le opportunità connesse alle tecnologie, di calarle nella propria realtà operativa e di avviare quei processi complessi di adattamento e riconfigurazione delle risorse dove la tecnologia è solo uno degli ingredienti e probabilmente non il più determinante.

D'altra parte, non deve sfuggire come un'efficace metabolizzazione delle tecnologie ICT possa diventare anche un fattore decisivo per alimentare le stesse *dynamic capabilities* delle imprese: il processo di qualificazione, il consolidamento ed il potenziamento dei sistemi informativi reso possibile dalle nuove tecnologie aumenta, infatti, la capacità dell'impresa di leggere il proprio ambiente competitivo, di sviluppare innovazioni veloci e di gestire il cambiamento. Viene, così, a crearsi un circuito virtuoso, per cui l'impresa dotata di *dynamic capabilities* è la più pronta a cogliere le opportunità legate all'ICT, ma questa prontezza diventa, al tempo stesso, un'occasione preziosa per aumentare le *dynamic capabilities* dell'organizzazione, aprendo nuovi interessanti scenari di sviluppo.

La circolarità virtuosa che viene a crearsi fra tecnologie ICT e competitività delle imprese rappresenta un'ottima ragione per cercare di comprendere le dinamiche che – incidendo sulla

creazione e sul mantenimento delle *dynamic capabilities* – consentono alle organizzazioni di trasformare le occasioni di innovazione in effettive opportunità di crescita. Ignorare questa dimensione può, infatti, portare l'impresa a ristagnare in una condizione di staticità che nel medio periodo ne comprometterà le performance strategiche ed operative, nonostante la presenza di continui investimenti in tecnologia, che nel migliore dei casi potranno produrre qualche modesto incremento di efficienza, ma difficilmente riusciranno a sostenere quel salto di qualità indispensabile per alimentare condizioni di innovazione continua.

3. Il rapporto complesso fra tecnologia e organizzazione

Il punto essenziale per comprendere la complessità dei processi di innovazione tecnologica è la consapevolezza del rapporto che viene a crearsi fra tecnologia ed organizzazione: un rapporto che sfugge a razionalizzazioni rigide e che spesso segue logiche difficilmente prevedibili e programmabili.

La letteratura organizzativa, fin dagli anni '80, quando la rivoluzione della società dell'informazione muoveva i primi passi, ha individuato il problema e provato a fornire qualche utile chiave interpretativa. Si è evidenziato, infatti, come la tecnologia possa determinare importanti cambiamenti nelle strutture organizzative alterando i ruoli istituzionali e i modelli di interazione (Barley, 1986). Tali cambiamenti non possono essere letti come una fisiologica e prevedibile conseguenza dell'introduzione di una specifica tecnologia, ma nascono da una complessa interazione che viene a crearsi fra le artefatti tecnologici, procedure operative, dinamiche sociali, riferimenti culturali. L'azione combinata di questi diversi fattori produce effetti difficilmente ipotizzabili a priori e spesso lontani da quelli pianificati, che arrivano a toccare dimensioni e dinamiche non sempre immediatamente riconducibili all'innovazione tecnologica introdotta.

La tecnologia, infatti, determina modifiche ai processi organizzativi e alle procedure, rende disponibili informazioni prima ignote, favorisce l'accesso a dati prima nascosti ai più, agevola la misurazione tempestiva delle performance, modifica il profilo di competenze necessarie per svolgere alcune mansioni, apre nuovi canali di comunicazione. Tutto questo si traduce in un'alterazione degli equilibri di potere, rende obsolete soluzioni organizzative profondamente radicate e costringe tutti gli attori della vita aziendale e rivedere le proprie posizioni e i propri comportamenti.

Si comprende, quindi, come l'introduzioni si tecnologie simili in contesti organizzativi differenti possa produrre risultati del tutto diversi: la tecnologia rappresenta, infatti, solo uno degli innumerevoli ingredienti che entrano in gioco nella complessa "reazione" del sistema organizzativo, dove si intrecciano dinamiche sociali solo in parte palesi e atteggiamenti individuali legati a dimensioni psicologiche spesso difficili da decifrare. L'impegno di quanti si trovano coinvolti in progetti di innovazione basati su nuove tecnologie non può, quindi, limitarsi alla semplice pianificazione di un processo di adozione più o meno strutturato, ma dovrà estendersi al monitoraggio e al controllo dell'impatto che l'introduzione della tecnologia andrà a determinare sulle strutture e sulle prassi in vigore all'interno dell'azienda (Blau et al., 1976; Barley, 1988; Orlikowski 1992).

Il rapporto fra le componenti "materiali", che rappresentano la manifestazione tangibile della tecnologia, e quelle "umane", che costituiscono il cuore di ogni processo organizzativo, deve essere studiato ricorrendo ad un approccio che ne colga in pieno tutte le dinamiche sistemiche (Leonardi, Barley, 2008). Occorre superare la prospettiva che, pur riconoscendo le relazioni esistenti fra tecnologia e variabili organizzative, tende a valutare l'impatto delle prime sulle seconde mediante una logica unidirezionale e tendenzialmente deterministica, per esplorare in tutte la sua complessità la rete di interdipendenze che lega insieme tutte le variabili in gioco (*costitutive entanglement*). Si può parlare, in tal senso, di una prospettiva di analisi "socio-materiale" (Orlikowski, 2007), dove gli artefatti della tecnologia (attrezzature, hardware, software, ecc.) entrano a far parte a pieno titolo del sistema organizzativo intrecciandosi con le attività umane e le passi operative, fino a diventare una componente costitutiva all'interno di specifici contesti sociali, storici, politici e culturali.

4. Il cuore del problema: le routine organizzative

Le considerazioni proposte dalla letteratura organizzativa offrono una chiave interpretativa efficace per spiegare il fallimento di molti progetti di implementazione di nuovi software che pure sono circondati da grandi aspettative e portati avanti con un buon livello di commitment da parte del management. In molti casi il problema non dipende da una cattiva progettazione del processo di implementazione, che viene programmato con cura, prestando la dovuta attenzione sia alle fasi propedeutiche (analisi dei fabbisogni, definizione delle specifiche) sia a quelle successive al deploy dell'applicazione (formazione, fine tuning degli applicativi). Nonostante queste attenzioni, infatti, le "reazioni" dell'organizzazione risultano spesso diverse da quelle previste e l'innovazione produce effetti indesiderati o comunque deludenti rispetto alle aspettative e agli sforzi profusi dal punto di vista finanziario ed organizzativo.
In realtà, la qualità della progettazione del processo di innovazione tecnologica è fondamentale, ma non è sufficiente, soprattutto quando l'innovazione va ad incidere sui processi *core* dell'azienda, dove sono maggiormente radicate le routine organizzative e dove il cambiamento è destinato a dover rimuovere più elevati fattori di resistenza ed inerzia. Per comprendere le ragioni di questi insuccessi che spesso frustrano l'impegno del management e dei responsabili dei reparti IT è fondamentale proprio il concetto di "routine", spesso richiamato nel linguaggio manageriale, ma quasi altrettanto spesso frainteso.
Si tratta, infatti, di un concetto complesso che va compreso fino in fondo, se si vogliono evitare ambiguità che non si estendono solo al campo della speculazione teorica, ma determinano conseguenze pratiche di grande portata (Pentland, Feldman, 2008). L'equivoco di fondo è quello di confondere le routine "morte" (*dead routines*), ovvero quelle formalmente definite attraverso la realizzazione di artefatti (diagrammi, software, manuali delle procedure, ecc.) con le routine "vive" (*live routines*), quelle agite dal personale effettivamente coinvolto nei processi operativi (Cohen, 2007). La differenza fondamentale fra le due è che le prime sono disegnate a tavolino da persone che progettano e pianificano con una conoscenza generalmente indiretta e parziale della realtà, mentre le seconde sono vissute quotidianamente da persone impegnate in uno sforzo costante di *problem solving* chiamato a gestire problemi non previsti, facendo

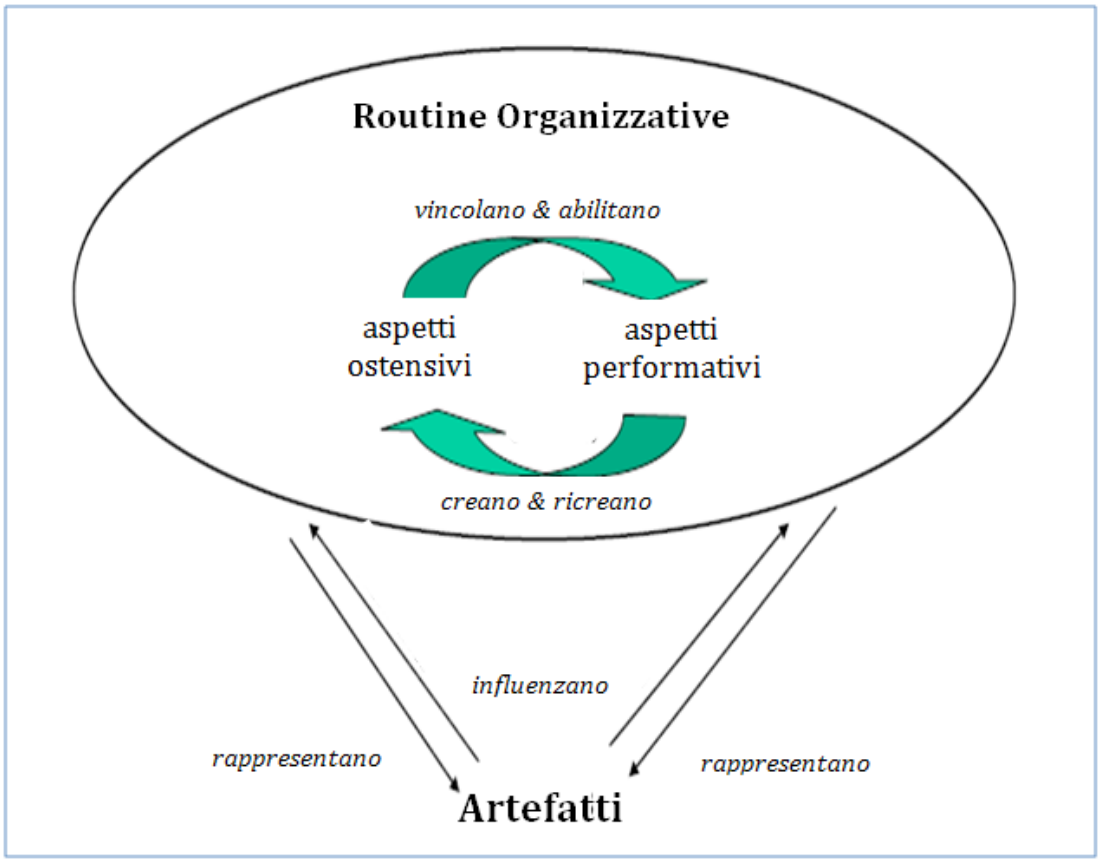
affidamento sulle proprie capacità di apprendimento.
Tenendo conto di questa duplice chiave di lettura, le routine possono essere definite come "sistemi generativi che possono produrre un'ampia varietà di risultati in relazione alle circostanze"[1]. In questa prospettiva la routine emerge come il prodotto complesso di regolarità ed aspettative astratte che orientano il comportamento dei partecipanti (*aspetti "ostensivi"*)[2] ed i comportamenti effettivi realizzati da persone specifiche in momenti specifici (*aspetti "performativi"*): due momenti mutualmente interdipendenti che consentono di riconoscere i modelli ripetitivi di azione in cui prende forma la routine organizzativa (Feldman, Pentland, 2003).
Il concetto che emerge è, pertanto, di natura complessa: da una parte, gli aspetti ostensivi (ciò che le persone pensano di dover fare) abilitano, orientano e vincolano quelli performativi (ciò che le persone effettivamente fanno); dall'altro, questi ultimi creano e ricreano continuamente i primi, modificando la percezione degli attori sulla base dell'apprendimento maturato nell'azione (*learning by doing*). In questo rapporto dialettico, il ruolo degli "artefatti" - fra cui si inseriscono a pieno titolo i software e gli strumenti ICT, ma anche i più tradizionali manuali delle procedure - rimane "esterno" nel senso che essi influenzano e rappresentano la routine, ma devono essere considerati "altro" da essa (figura 1).
Gli artefatti possono, infatti, riflettere sia gli aspetti ostensivi della routine (si pensi, ad esempio, ad una procedura formalizzata) che quelli performativi (come nel caso delle registrazioni di eventi su un database). In questo senso essi possono influenzare la routine, in quanto forniscono delle linee guida o dei vincoli operativi, ma – a meno che non si tratti di processi completamente automatizzati – lasciano aperta un'ampia possibilità di scelte alternative nella realizzazione dei comportamenti effettivi. Ed è proprio in questo "spazio" che si inserisce la discrezionalità dei singoli attori organizzativi, i quali tenderanno ad assumere comportamenti differenziati in relazione alle proprie aspettative, alle percezioni personali e alle circostanze concrete in cui si troveranno ad operare.

---

[1] Traduzione della definizione proposta da Pentland e Feldman (2008) che si riferiscono alle "live routines" come a "generative systems that can produce a wide variety of performances" (Pentland, Feldman, 2008, p. 241).

[2] Altri autori preferiscono parlare di "disposition" (disposizione) (Becker, 2004). Non bisogna, però, pensare che gli aspetti ostensive siano le regole o le procedure scritte, che in molti casi nemmeno esistono: sono, piuttosto, le percezioni che i partecipanti hanno dei compiti loro assegnati. In tal senso gli aspetti ostensivi possono variare anche all'interno della stessa organizzazione, in quanto le percezioni possono essere differenziate fra i vari attori coinvolti nella routine.

Figura 1: Le routine organizzative come sistemi generativi



Fonte: Adattamento da Pentland, Feldman, 2008

Il management deve, quindi, evitare l'errore di considerare il design degli artefatti e, in particolare, quello dei nuovi sistemi software come il passaggio fondamentale e autonomamente sufficiente per produrre cambiamenti organizzativi. Questo non avverrà o, almeno, non sempre avverrà nella direzione e nella misura desiderate, se non si sarà capaci di intervenire anche sulle routine "vive" che, di fatto, costituiscono l'anima di ogni organizzazione. In questo senso, non sempre aiutano le logiche tipiche di molti approcci consulenziali di moda, come il *Business Process Reengineering* (BPR) o il *Business Process Management* (BPM) dove l'enfasi è posta tutta sul "disegno" dei processi in una prospettiva di tipo top-down che vede l'organizzazione come una materia plastica, facilmente modellabile sulla base di valutazioni razionalistiche, dove artefatti ed essere umani dovrebbero combinarsi in incastri perfetti, tanto più improbabili quanto più i processi sfuggono all'opportunità di una piena automazione.

5. Conclusioni: intervenire sulle routine per gestire il cambiamento

La consapevolezza della natura complessa delle routine organizzative rappresenta una condizione fondamentale per gestire con efficacia i progetti di innovazione basati sulle tecnologie dell'informazione e della comunicazione. Partendo da tale consapevolezza sarà, infatti, possibile costruire percorsi di innovazione realmente attenti alle dinamiche organizzative e, quindi, capaci di sostenere quel processo di cambiamento che rappresenta il cuore delle *dynamic capabilities, vera fonte di ogni vantaggio competitivo durevole.*

In quest'ottica, è opportuno che tali processi siano sviluppati attraverso un coinvolgimento attivo del personale che preveda momenti di formazione e pratica congiunta sul campo, un po' come accade nelle prove d'orchestra, dove lo spartito (artefatto) è un punto di partenza ma è solo attraverso l'esercizio musicale ripetuto in comune che si arriva a costruire una piena condivisione sulle modalità di attuazione della performance collettiva (dimensione ostensiva della routine). Allo stesso modo, le imprese dovrebbero moltiplicare le occasioni di formazione, di sperimentazione, di confronto reciproco, così da calare le tecnologie innovative nella quotidianità della vita organizzativa e contribuire all'evoluzione positiva delle routine che i nuovi artefatti sono in grado di alimentare. Potranno, così, emergere i diversi punti di vista degli attori del processo, i loro interessi, le loro aspettative, le alternative di azione considerate, rendendo possibile la creazione di sistemi di incentivi efficaci, molto più funzionali rispetto all'obiettivo di promuovere i comportamenti desiderati di quanto non lo siano software che "costringono" gli operatori a seguire procedure rigide.

Le persone coinvolte nei processi operativi non devono, quindi, essere considerate come parti di meccanismi quasi automatici che comprimono drasticamente gli spazi di discrezionalità, ma come soggetti pensanti, capaci di iniziativa, che non si limitano ad eseguire compiti definiti a priori ma possono avere un ruolo attivo nel costruire nuove routine. Il comportamento "deviante" non deve essere vissuto come una violazione delle regole aziendali, ma deve essere studiato al fine di valutare le logiche che lo determinano e verificare il valore che può produrre, magari tracciando la via per una nuova routine più efficiente ed efficace.

Questi accorgimenti potranno avere un ruolo decisivo per produrre una reale innovazione a partire dall'introduzione di nuove soluzioni basate sulle tecnologie ICT. Queste ultime, infatti, non saranno viste come una panacea universale calato dall'alto per aumentare la produttività e la qualità del lavoro, bensì come un ulteriore elemento che viene ad introdursi in un complesso sistema socio-materiale, dove uomini e artefatti interagiscono in maniera spesso non prevedibile, creando e ri-creando ogni giorno nuove routine che, nel loro insieme, alimentano il know how organizzativo su cui si basa la competitività delle imprese. In questo modo potranno essere evitate aspettative eccessive e ingenue generalmente associate all'introduzione di nuove tecnologie e potrà essere sfruttato tutto il potenziale cognitivo che già risiede nell'organizzazione, valorizzando le risorse presenti e sostenendo lo sviluppo di dynamic capabilities.

BIBLIOGRAFIA

Barley S. R. (1986), "Technology as an Occasion for Structuring: Evidence from Observations of CT Scanners and the Social Order of Radiology Departments", *Administrative Science Quarterly*, n. 31, pp. 78–108.

Barley S. R. (1988), "Technology, power, and the social organization of work", *Research in the Sociology of Organizations*, n.6, pp. 33-80.

Barney J.B. (1991), "Firm resources and sustained competitive advantage." *Journal of Management*, n. 17, pp. 99-120.

Becker M. C. (2004), "Organizational routines: A review of the literature", *Industrial and Corporate Change*, n. 13, pp. 643–678.

Blau P. M., Falbe C. M., McKinley W., Tracy P. K. (1976), "Technology and organization in manufacturing", *Administrative Science Quarterly*, n. 21, pp. 20–40.

Cohen, M.D. (2007), "Reading Dewey: Reflections on the study of routine", *Organization Studies*, n. 28, 773–786.

D'Aveni R. (1995), *Ipercompetizione. Le nuove regole per affrontare la concorrenza dinamica*, Il Sole 24 Ore Libri, Milano.

Feldman, Pentland (2003), "Reconceptualizing organizational routines as a source of flexibility and change", *Administrative Science Quarterly,* n. 48, pp. 94–118.

Grant R.M. (1991), "The Resource Based Theory of Competitive Advantage: Implications for Strategy Formulation", *California Management Review*, vol. 33, 3.

Helfat C., Finkelstein S., Mitchell W., Peteraf M.A., Singh H., Teece D.J., Winter S.G. (2007), *Dynamic Capabilities: Understanding Strategic Change in Organizations*, Blackwell: Oxford, U.K.

Leonardi, P., & Barley, S. R. (2008). "Materiality and change: Five challenges to building better theory about technology and organizing", *Information and Organization*, n. 18, pp. 159–176.

Management Journal, n. 25, pp. 465-499.

Mintzberg H. (1994). *The Rise and Fall of Strategic Planning*, Prentice Hall, London, Eng.

Mintzberg H., Waters, J.A. (1982), "Tracking strategy in an entrepreneurial firm", *Academy of*

Orlikowski W.J. (2007), "The duality of technology: Rethinking the concept of technology in organizations". *Organization Science*, n. 3/3, pp. 398–427.

Orlikowski, W.J. (1992), "The duality of technology: Rethinking the concept of technology in organizations'. *Organization Science*, 3/3, pp. 398–427.

Pentland B.T., Feldman M.S. (2008), "Designing routines: On the folly of designing artifacts, while hoping for patterns of action", *Information and Organization*, n.18, pp. 235–250.

Peteraf M.A. (1993), "The cornerstones of competitive advantage: a resource-based view", *Strategic Management Journal*, Vol. 14, No. 3, pp. 179–191.

Prahalad C.K., Hamel G. (1990) "The core competence of the corporation", *Harvard Business Review*, v. 68, no. 3, pp. 79–91.

Rullani E. (2004), *La fabbrica dell'immateriale: produrre valore con la conoscenza*, Carrocci, Roma.

Rullani E. (2006), "L'internazionalizzazione invisibile. La nuova geografia dei distretti e delle filiere produttive", *Sinergie*, n. 69, pp. 3-32,.

Rumelt, R P. (1991), "How much does industry matter?", *Strategic Management Journal*, Vol. 12, No. 3, pp. 167–185

Teece D.J., Pisano G, Shuen A. (1997). "Dynamic capabilities and strategic management", *Strategic Management Journal*, vol. 18, n. 7, pp. 509–533.

Teece D.J., Pisano G., (1994), "The dynamic capabilities of firms: an introduction", *Industrial and Corporate Change*, Vol. 3, pp. 537-556.

Vicari S. (1991), *L'impresa vivente*, Etas, Milano, 1991.

Wernerfelt B. (1984), "A resource-based view of the firm". *Strategic Management Journal*, Vol.5, pp. 171–180.

Winter S.G. (2003), "Understanding dynamic capabilities", *Strategic Management Journal*, October Special Issue, n.24, pp. 991–996.

Rivista elettronica di Diritto, Economia, Management

N. 1 - 2010 · pp. 192-212

Diritto alla salute e politiche di sviluppo dei servizi sanitari digitali

Gianpasquale Preite

Abstract: During the last decade the Italian health policy has been the subject of many administrative and constitutional reforms giving it its current federalist direction. Such a direction legitimizes the introduction of new regional organizational patterns as well as changes concerning ownership on administrative and policy responsibility, with impacts on both health services quality and expenditure reduction. Considering where we started and moving from the evolution of e-health services, the article aims at analyzing the organization of healthcare systems within the widest issue pertaining to both quality and digital health services, analyzed through a risk management methodology that uses integrated technologies (ICTs) to support decision-making processes. Therefore, the perspective embraced in this article aims at pointing out the operating modes of a health pattern able to create economies of scales, guarantees for inmates, healthcare professionals as well as the organizational structure with positive impacts on the public system.

Parole chiave: Politica sanitaria, diritto alla salute, e-Health, federalismo, patrimonio informativo, rischio clinico, sistema documentale, cartella clinica informatica.

Introduzione

Il sistema sanitario italiano, ha vissuto negli ultimi anni un processo di profondo cambiamento che si inquadra nel nuovo modello di ordine sociale definito dalla società dell'informazione. Si è trattato, infatti, di una complessiva riforma della pubblica amministrazione finalizzata a snellire processi e procedimenti, a razionalizzare le decisioni di spesa, a migliorare i servizi al cittadino, a rendere trasparente l'azione amministrativa.
In tale contesto, il diritto alla salute si configura come una fattispecie eterogenea nella quale s'iscrivono istanze di natura politica, giuridica, finanziaria, ambientale, medica, etica e tecnologica. Ciò implica una serie di diritti presupposti: diritto alla vita, diritto alla dignità, diritto di

Articolo pervenuto il 28 settembre 2010, approvato il 20 novembre 2010

cittadinanza; e derivati: diritto alle prestazioni sanitarie, diritto all'uso delle tecnologie, diritto all'autodeterminazione informativa e informatica, diritto alla privacy, diritto del paziente a ricevere tutte le informazioni relative ai trattamenti cui deve sottoporsi, diritto a esprimere il proprio consenso al trattamento, diritto al reclamo e al risarcimento, diritto di accesso alla propria cartella clinica, diritto ad una *second opinion* (Toth 2009, 80-81). L'eguaglianza e l'imparzialità di trattamento sancite dalla costituzione si collocano, dunque, nell'area del bilanciamento tra bisogni sanitari e allocazione di risorse scarse, da cui consegue la necessità di selezionare le priorità sanitarie di un sistema.

Nell'ultimo decennio la politica sanitaria italiana, al pari di tutte le altre politiche pubbliche, è stata profondamente modificata da riforme amministrative e costituzionali che hanno delineato la sua attuale direzione in senso federalista. Ciò ha reso possibile l'introduzione di nuovi modelli organizzativi a dimensione regionale e modifiche nella titolarità delle responsabilità amministrative e politiche, con effetti sulla qualità dei servizi sanitari e sul contenimento dei costi. Parallelamente, anche il rapporto tra sanità, cittadino e impresa ha subito un sostanziale cambiamento derivante da due fenomeni concomitanti: da un lato è cresciuta la domanda di servizi complessi e tecnologicamente avanzati; dall'altro lato è emerso il riconoscimento della strumentalità aziendale come criterio di riferimento per superare il modello organizzativo burocratico e legittimare i principi di efficienza, efficacia ed economicità auspicati dal federalismo e ritenuti indispensabili per misurare l'attività delle regioni e per garantire la competitività del sistema sanitario.

Come osserva Freddi (2009), la discussione contemporanea sulle politiche sanitarie coinvolge numerosi paradigmi teorici e orientamenti metodici; ma pur in presenza di tale pluralità, la questione centrale si concretizza su tre problemi altamente interconnessi: accesso di massa, qualità della medicina e contenimento della spesa, ed è rispetto a quest'articolazione che l'intervento pubblico nella sanità è una ineludibile necessità.

Alla luce di queste premesse e partendo dall'evoluzione dei servizi e-health, il presente contributo si propone di analizzare l'organizzazione delle strutture sanitarie nell'ambito della più generale questione riguardante la qualità e la sicurezza dei servizi sanitari digitali. Infatti, attraverso l'impiego di tecnologie integrate (ICTs) a supporto dei processi decisionali e di controllo (Clinical Decision Support System, Health Technology Assessment, Clinical Data Repository, Electronic Medical Record), è possibile sostenere il passaggio da una prospettiva di gestione degli eventi sfavorevoli a una prospettiva di gestione del rischio, contenimento dei costi e riduzione del contenzioso; in altri termini il passaggio da un sistema esclusivamente reattivo (gestione della non conformità, gestione delle emergenze ecc.) a un sistema prevalentemente pro-attivo e preventivo (a titolo esemplificativo, si pensi al vantaggio economico e giuridico, di tracciare e certificare dati e informazioni sui pazienti e sui servizi erogati dalle strutture, in modo che gli stessi risultino accessibili da qualsiasi struttura autorizzata, protetti contro accessi non autorizzati, perdita e/o diffusione illecita, errori sulla refertazione, somministrazione di farmaci e prescrizioni di varia natura).

La prospettiva assunta si propone, pertanto, di evidenziare le modalità di funzionamento di un modello sanitario organizzato per l'erogazione di servizi digitali, e capace di generare economie di scala con ricadute positive sul più ampio processo di attuazione del federalismo fiscale, oltre che assicurare maggiori garanzie per i pazienti, gli operatori sanitari e la stessa struttura organizzativa.

1. Evoluzione politica e sociale del diritto alla salute

Nel corso degli ultimi cinquant'anni la tutela della salute, intesa nella sua più vasta accezione, ha progressivamente acquisito una dignità pari alla tutela della libertà; infatti, oltre che di espressa previsione costituzionale si tratta di un valore universalmente riconosciuto. Tuttavia, a differenza della tutela della libertà, rispetto alla quale si postula un comportamento garantistico e immediatamente precettivo da parte dell'autorità statale, la tutela della salute, considerata come sviluppo e completamento della prima, presuppone un approccio che coinvolge contestualmente volontà giuridica e volontà politica (Luciani 1991).

La salute è, senza dubbio, un diritto della personalità, nel quale maggiormente si rispecchia la generale vocazione costituzionale nei riguardi della persona umana (Cocconi 1998, 38). Proprio per questo, la tutela della salute rientra tra i compiti fondamentali che la Costituzione assegna alla Repubblica, secondo quanto disposto dall'art. 32, comma 1, che recita: *"La Repubblica tutela la salute come fondamentale diritto dell'individuo e interesse della collettività, e garantisce cure gratuite agli indigenti"*. Dall'accurata lettura della norma emerge una fondamentale considerazione, ossia, che nel nostro ordinamento il diritto alla salute gode della più ampia e piena tutela sia sotto il profilo della portata normativa, che sotto il profilo dell'effettiva tutela. In relazione al primo aspetto, si rileva che il diritto alla salute è ricompreso tra i diritti fondamentali e come tale è riconducibile al rango dei diritti inviolabili contenuti nell'art. 2 della Costituzione[1] (Predabissi 2009, 13). L'ordinamento italiano non si limita soltanto a riconoscere l'inviolabilità del diritto in esame, bensì pone l'obbligo in capo allo Stato di rimuovere ogni forma di ostacolo e disparità sociale nell'esplicazione del diritto alla salute, propria della visione "individuale" voluta dall'art. 32 della Costituzione.

Sulla scorta di questa impostazione, la decisione di istituire un Servizio Sanitario Nazionale ha coinciso con la volontà di eliminare quel sistema mutualistico proprio degli anni Settanta, fonte di tutele eccessivamente differenziate e condizionate dallo status sociale e lavorativo dei singoli pazienti, per affermare un sistema conforme alla *ratio* costituzionale in cui tutti gli individui, cittadini, lavoratori, non abbienti, possano ottenere una tutela indifferenziata. La vera svolta in questa direzione coincide con un importante intervento legislativo, l'emanazione della Legge n. 833/1978, che all'art. 1 dispone: *"la Repubblica tutela la salute come fondamentale diritto dell'individuo e interesse della collettività mediante il Sistema Sanitario Nazionale"*.

Dalla lettura del testo normativo emerge chiaramente la corrispondenza con il disposto costituzionale allorquando si ribadisce il ruolo primario e fondamentale del diritto alla salute e si afferma il valore sociale e democratico che il Sistema Sanitario Nazionale riveste, in quanto servizio che Stato, Regioni e Enti locali devono garantire alla collettività. A ciò si affianca la portata generale dell'art. 3, comma 2 della Costituzione, che prevede l'obbligo da parte dello Stato di rimuovere gli ostacoli di ordine economico e sociale che impediscono il pieno sviluppo della persona umana. Precetto costituzionale che delinea la necessità di un comportamento

[1] La ricostruzione storica del percorso seguito dall'Assemblea costituente, consente di compiere un ulteriore passaggio e affermare che il diritto alla salute tutelato dall'art. 32 rientri nel novero dei diritti inviolabili di cui all'art. 2 Cost., poiché conforme a quella valutazione volta ad individuare gli ambiti soggettivi giuridicamente rilevanti nel nostro ordinamento.

interventista dello Stato, volto a rimuovere le disparità sociali ed economiche e a porre le basi per un'uguaglianza sostanziale[2] (Pezzini 1998).
Nel quadro generale delle norme costituzionali in cui è ravvisabile la tutela al diritto della salute, vi è, infine, l'art. 23 secondo cui *"nessuna prestazione personale o patrimoniale può essere imposta se non in base alla legge"*. Tale norma introduce una riserva di legge assoluta nella previsione di trattamenti personali, ossia sanitari, da eseguire obbligatoriamente sulla persona e che fa emergere la necessità di adottare una visione unitaria dell'individuo tesa a coinvolgere la sua dimensione corporea, psichica e anche sociale. Il dettato costituzionale è rafforzato con il comma dell'art. 32 che, nella parte in cui si prevede il diritto alle prestazioni sanitarie, impone un comportamento attivo da parte dello Stato. A differenza, infatti, della tutela individuale del diritto alla salute, il valore precettivo contenuto nell'art. 32, connesso alla collettività, esige uno Stato interventista, in grado di garantire e predisporre i mezzi, le risorse umane, le attrezzature, gli ospedali e una struttura sanitaria tale da poter erogare efficienti ed efficaci servizi di assistenza e di prestazioni sanitarie, uniformi su tutto il territorio e che non tengano conto delle disparità economiche e sociali.
Il servizio sanitario è, dunque, da considerarsi un servizio pubblico obbligatorio ad attivazione necessaria, anche se non ne è imposta l'erogazione attraverso strutture pubbliche. Il precetto costituzionale correla in modo espresso situazioni soggettive di vantaggio degli amministrati, qualificate rispettivamente come "interesse" della collettività e come "diritto" fondamentale dell'individuo; ma, è in quest'ultima accezione che il diritto individuale alla salute si connota più precisamente come diritto sociale, ossia come pretesa positiva nei confronti del potere pubblico ad ottenere prestazioni sanitarie a tutela del bene salute. Il godimento pieno e compiuto di entrambe le situazioni di vantaggio enunciate rende necessaria l'intermediazione della legge, la quale deve disciplinare presupposti, contenuti e modalità dell'azione pubblica in campo sanitario, in modo tale da assicurare il perseguimento dei fini non rinunciabili prefissati dalla norma costituzionale (Cocconi 1998, 41 e ss.). In sintesi, in Italia, il diritto dei cittadini alla salute e all'assistenza sanitaria presuppone l'esistenza di un servizio pubblico obbligatorio, anche se il contenuto programmatico dell'art. 32 della Costituzione non può essere inteso come un riconoscimento del diritto alle prestazioni sanitarie in termini assoluti ed illimitati. Ed è per questo che, nella effettiva concretizzazione, il diritto alla salute, pur essendo ritenuto inerente e inscindibile dal riconoscimento della qualità di essere umano, risulta ben lontano dall'essere universalmente protetto, poiché nei singoli Stati e nelle singole legislazioni assume delle valenze differenti che, a seconda dei casi, riducono il diritto alla salute a diritto relativo (Corte Costituzionale, Sentenza 23 luglio 1992, n. 356, 2834 e ss.); ovvero economicamente determinato, dipendente dalla necessità di garantire l'equilibrio finanziario del sistema confrontandosi con la necessità di allocazione e selezione delle priorità sanitarie, causata dall'impossibilità economica di rispondere a tutti bisogni sanitari.
Di fatto, in sede di ridefinizione del rapporto tra «il diritto alla salute, per definizione incomprimibile e le risorse finanziarie, per definizione comprimibili» (Cavicchi 2005), si resta

[2] Il pieno sviluppo della persona esige, infatti, che "fondamentale" non sia soltanto la garanzia del libero godimento del bene, ma anche quella dell'effettivo godimento. Da qui dunque l'esigenza di un intervento attivo dello Stato per rimuovere gli ostacoli economici e sociali che si frappongono a tale effettivo godimento.

condizionati alla discrezionalità del legislatore, alla volontà politica[3] e al riconoscimento alle singole Regioni del potere di decidere come effettivamente ripartire le risorse distribuite in ambito nazionale (Borgonovi 1992), fondamentali per il bilanciamento degli elementi che il diritto alla salute comprende.
Un nuovo diritto che diventa benessere, vitalità, cittadinanza e non più mera assenza di malattia e che, pertanto richiede come contropartita, una quantità di risorse crescenti in risposta allo sviluppo tecnologico, all'evoluzione dei nuovi farmaci, all'invecchiamento crescente della popolazione e alla domanda stessa di salute come bene superiore, che aumenta più che proporzionalmente rispetto al PIL del Paese (Reviglio 2003, 73 e 74).

2. Gli effetti della riforma tra assistenza sanitaria e federalismo

Il decentramento avviato con la riforma del Titolo V e con la normativa susseguitasi in materia di federalismo fiscale, ha ridisegnato il volto delle politiche pubbliche. I sempre più stringenti vincoli, sia di natura squisitamente interna sia di origine comunitaria, hanno portato il legislatore statale e quello regionale a ridefinire la disciplina dei servizi sanitari (Romeo 2009) che, nell'ottica del contenimento della spesa, rappresentano uno dei settori più problematici, data l'inevitabile tensione tra l'esigenza di garantire il diritto alla salute e il rispetto dei numerosi condizionamenti finanziari dettati dall'esigenza della realizzazione del patto di stabilità interno (Peres 2002). Il legislatore ha, dunque, introdotto nuovi modelli organizzativi in sanità a dimensione regionale con significative modifiche nella titolarità delle responsabilità amministrative e politiche, con l'obiettivo di migliorare i servizi sanitari, contenere e ridurre i costi. Per questo, tra le principali cause degli interventi normativi, vi è la convinzione da parte del legislatore che l'attribuzione del potere decisionale e delle responsabilità finanziarie conseguenti (a livello locale) avrebbe potuto responsabilizzare maggiormente gli amministratori pubblici verso comportamenti di spesa virtuosi (Dirindin 2001; Pisauro 2002).
Ma, con l'avvento del federalismo, si ha una tensione tra la tutela della salute prevalentemente a carico delle Regioni e quella dei livelli essenziali di assistenza, di competenza esclusiva dello Stato. Il principio che caratterizza il progetto contenuto nella legge n. 42/2009 è quello del superamento, per ogni livello di governo, del criterio del finanziamento della spesa storica. Per i livelli essenziali delle prestazioni che devono essere garantiti su tutto il territorio nazionale e per le funzioni fondamentali degli Enti locali, esso sarà sostituito da un criterio di finanziamento della spesa efficiente, basato sulla copertura completa del fabbisogno standard. Per le altre spese, il criterio della spesa storica verrà sostituito da un ravvicinamento delle capacità fiscali.
In tale contesto si rivela, ancora una volta, l'intrinseca ambiguità dell'espressione dei "livelli essenziali" che il servizio deve garantire, poiché se per essenzialità si intende un "contenuto

[3] Con la legge finanziaria si decidono le risorse da destinare al sistema sanitario nazionale e la definizione degli ambiti concreti di garanzia

minimo", questo produrrebbe ulteriori disparità di trattamento territoriali a causa degli squilibri nella distribuzione della ricchezza fra le diverse aree del Paese.
Per le spese riconducibili ai livelli essenziali delle prestazioni e alle funzioni fondamentali, laddove le fonti di entrata assegnata a Regioni ed Enti locali non siano sufficienti a coprire il fabbisogno standard, interverrà la perequazione.
L'individuazione del costo e del fabbisogno standard per le varie funzioni, rinviata ad uno dei decreti legislativi, costituisce anch'essa un passaggio cruciale che può pregiudicare il successo della riforma. V'è, infatti, il rischio che il negoziato politico porti a fissare il fabbisogno ed il costo standard a livelli troppo alti, eliminando gli incentivi dall'efficienza della spesa.
Per le funzioni diverse da quelle sopra indicate, la legge non prevede garanzie di finanziamento: ciascun livello di governo dovrà, pertanto, provvedere con la propria capacità fiscale. Tuttavia, sarà assicurata una perequazione per "ridurre adeguatamente" le differenze tra territori per le Regioni con minore capacità fiscale, identificate come le Regioni con gettito per abitante di una specifica addizionale Irpef inferiore alla media nazionale. Si tratta, quindi, di una perequazione parziale. La legge richiede che essa non alteri l'ordine tra i territori in termini di capacità fiscali e ne impedisca la modifica nel tempo, in conseguenza dell'evoluzione del quadro economico territoriale.
Il cambiamento prospettato dalla riforma risulta, dunque, ancora in fieri a causa di un "disallineamento" normativo che caratterizza la fase di transizione connessa a continue contrattazioni in sede di Conferenza Stato-Regioni sia per l'identificazione dell'ammontare delle risorse del bilancio statale da destinare alla sanità, che per la loro ripartizioni secondo criteri annualmente modificati. D'altro canto un'interpretazione estensiva dei livelli essenziali condurrebbe a una fissazione fra il potere di determinazione degli standard di pertinenza statale e l'onere di individuare i mezzi di copertura finanziaria spettante alle Regioni.
Siamo in una fase di transizione legislativa e di confusione dei ruoli istituzionali, in cui la giurisprudenza della Corte Costituzionale rappresenta un punto di riferimento importante.
Il trend della spesa sanitaria rispetto al PIL evidenzia omogeneità e si caratterizza per una forte crescita seguita da un decremento, frutto della dinamica della spesa pubblica (Caroppo, Turati 2007).
Se negli anni novanta del secolo scorso si è assistito ad una forte frenata della spesa sanitaria, grazie agli interventi di riforma che hanno aziendalizzato il Servizio sanitario, in quest'ultimo decennio si è avuto, invece, un forte incremento della spesa sanitaria ad un ritmo superiore rispetto all'economia, dovuto all'aumento dei consumi pro capite e alla crescita tendenziale dei prezzi relativi delle prestazioni sanitarie. A questa tendenza si associa la difficoltà dei governi nazionali di inasprire il carico fiscale e, quindi, di incettare nuove risorse da destinare al sovvenzionamento della spesa pubblica.
L'affermarsi del principio di sussidiarietà di origini comunitarie, poi, ha reso l'intervento dello Stato meramente "eventuale", ovvero realizzabile solo nell'ipotesi in cui le politiche attuate dai governi sub statali si rivelino incapaci di portare avanti con efficacia ed efficienza i compiti ad essi direttamente spettanti. Da ciò scaturiscono una serie di problematiche, nel comparto sanitario, circa il coordinamento e/o la "sostituzione" dello Stato con gli enti pubblici territoriali di fronte all'incremento della domanda (eterogenea a livello territoriale) e alla richiesta di maggiore di qualità del servizio (anch'essa difficilmente standardizzabile), rispetto

alle risorse necessarie per poterla supportare. Il sistema di protezione sociale dell'individuo diventa così meno forte e più selettivo. Trova sempre maggiore spazio il concetto di comunità solidale (welfare community), che sostituisce quello di stato sociale. Si prevede, inoltre, la dilatazione della quota privata della spesa sanitaria.

Il cambio di rotta nel sistema di finanziamento dal 2001, avvenuto con l'introduzione del federalismo fiscale, ha ridisegnato l'assetto della sanità pubblica. In precedenza, infatti, il Servizio Sanitario Nazionale veniva finanziato calcolando il fabbisogno nazionale sulla base dei livelli essenziali di tutela sanitaria e si determinava il fabbisogno regionale sulla quota capitaria ponderata (Franco, Zanardi 2003). Quest'ultimo veniva coperto per il 90% dal gettito dell'Irap e per la parte residuale dal Fondo Sanitario Nazionale.

La nuova normativa ha affidato il finanziamento della sanità alla finanza regionale complessiva senza vincoli di destinazione ad eccezione di una quota utilizzata per programmi o finalità particolari gestita centralmente. Al di là di come avviene materialmente questa modifica del regime di erogazione dei capitali necessari per la spesa sanitaria, è importante notare che è previsto l'avvio di un sistema di monitoraggio dei livelli essenziali di assistenza offerti da ciascuna Regione, il cui mancato rispetto comporta delle sanzioni che possono interessare i trasferimenti perequativi.

Tuttavia, non è così scontato credere che per migliorare l'efficienza e la qualità del servizio offerto, tenendo conto delle specificità locali e delle differenti preferenze, sia necessario devolvere l'intera competenza di legiferare in materia. Devolvere alle Regioni la competenza esclusiva in materia di politica sanitaria, ad esempio, potrebbe invece voler dire non guardare solo all'organizzazione del servizio, ma ai contenuti politici degli indirizzi da seguire, enfatizzando maggiormente lo status di cittadino regionale piuttosto che l'interesse nazionale e, anche se si ritiene esistano esternalità in materia, trascurarne l'importanza.

Questo processo di cambiamento istituzionale presenta costi e benefici per la collettività e per le amministrazioni chiamate ad attuare le riforme. Da un lato potrebbe non riuscire a contenere i livelli di spesa e razionalizzare i costi della pubblica amministrazione, visto che l'impiego delle risorse finanziarie nel complesso non sembra diminuire; d'altro lato, potrebbe consentire una maggiore attenzione alle necessità locali, differenziando, così come nei propositi in fondo condivisibili, dei processi di decentramento, interventi e misure politiche in modo che corrispondano maggiormente al profilo del territorio in esame.

Appare tuttavia complicato il tentativo di conciliare questo interesse locale, che è l'essenza di tutte le riforme in senso federalista, con la tutela e salvaguardia di un interesse nazionale. Di recente, forse in risposta alla crescente domanda di federalismo degli ultimi anni, l'attenzione al concetto di interesse nazionale, che appare strettamente collegato al concetto di cittadinanza nazionale, sembra sempre più marcata. Questo per evitare, probabilmente, che eccessive differenziazioni nell'organizzazione possano portare all'individuazione di diverse finalità politiche, diverse priorità e modalità per raggiungere gli obiettivi prefissati.

Un certo grado di uniformità, infatti, aiuta a garantire, sull'intero territorio nazionale il diritto e l'accesso ad alcuni servizi previsti dalla Costituzione e perciò ritenuti fondamentali; e accanto a considerazioni soggettive, quali l'importanza che evidentemente ognuno di noi può attribuire alla cittadinanza e solidarietà nazionale piuttosto che regionale, possono essere presi in esame aspetti economici, quali, ad esempio, la promozione dell'efficienza allocativa (France 2006).

Non si comprende ancora chiaramente se queste criticità potranno essere risolte con l'attuale riforma, che mantiene come competenza concorrente (o esclusiva dello Stato) la tutela della salute, ma prevede che l'assistenza e l'organizzazione sanitaria diventi una competenza esclusiva delle Regioni. Difficile avanzare ipotesi, probabilmente si avrebbero riflessi soprattutto in termini di finanziamento delle politiche, nel caso in cui, a fronte di un aumento di competenze da svolgere, si rivendicassero maggiori coperture finanziarie. In questo caso, si evidenzierebbero in tutta la loro gravità i profondi divari esistenti tra i bilanci regionali. Sebbene non siano disponibili cifre ufficiali circa i costi complessivi dei Livelli essenziali di assistenza, è possibile avanzare alcune riflessioni circa i comportamenti differenti adottati dalle Regioni per ripianare il disavanzo sanitario derivante dal mancato contenimento delle risorse stanziate.

In effetti, sembrano emergere i primi squilibri, o quanto meno le prime differenziazioni politiche, sul territorio nazionale. Infatti, le Regioni più ricche (in prevalenza del nord Italia) sono ricorse soprattutto a strumenti di inasprimento fiscale, coscienti di poter contare su un robusto bacino d'entrata; le Regioni del sud, invece, hanno adottato un altro tipo di politica, quella del contenimento delle spese. Accanto a valutazioni positive di un atteggiamento che comunque può portare a ridurre sprechi o inefficienze, è necessario tenere sotto controllo il rischio che questo si trasformi in una modifica al ribasso del livello di erogazione del servizio che potrebbe avere riflessi rilevanti per il mantenimento di standard nazionali, pregiudicando il principio di equità su tutto il territorio nazionale, dal momento che ci sono cittadini che, per motivi di stabilità di bilancio, ricevono probabilmente trattamenti differenti in risposta a situazioni omogenee.

Pertanto, fino a quando si riterrà di analizzare il problema cercando di definire "geometricamente" competenze e ruoli, si finirà per proporre soluzioni solo apparentemente semplificatrici. Infatti, qualunque sia la portata o le sfumature di cambiamento che avrà il nuovo assetto costituzionale, sembra permanere l'esigenza di mantenere una cornice comune di diritti e di erogazioni pubbliche pur nella salvaguardia delle specificità regionali. A fronte di tensioni crescenti tra decentramento da una parte ed esigenza di standard nazionali e integrazione politica dall'altra, appare sempre più necessaria la creazione di un sistema di coordinamento tra lo Stato e le Regioni, sul modello del coordinamento aperto. Lo Stato fissa annualmente le linee guida da adottare da parte regionale (senza dimenticare la partecipazione necessaria degli Enti locali) e queste predispongono a loro volta i piani di azione con cui fissare obiettivi coerenti e compatibili con le linee guida nazionali indicando le strategie per raggiungerli, oltre che lo stato di realizzazione degli obiettivi fissati in precedenza.

A livello europeo, tuttavia, è già da alcuni anni che ci si interroga più a fondo sulla bontà del decentramento e sull'utilità di ri-accentrare in capo al governo nazionale almeno alcune competenze, senza necessariamente privare di responsabilità i governo sub-nazionali. Al di là delle diverse soluzioni e combinazioni possibili, in tempi di risorse scarse e di crescita della domanda di cura e assistenza, il tema dei rapporti tra livelli decisionali continuerà ad essere esplorato (Maino 2009, 94) al fine di giungere a soluzioni che soddisfino, simultaneamente, il contenimento della spesa pubblica e la qualità nell'erogazione dei servizi sanitari.

3. Il processo di riforma dall'interno delle strutture sanitarie: organizzare l'e-health

Indipendentemente dagli sviluppi che l'attuazione del federalismo in Italia potrà seguire e degli impegni programmatici che le Regioni assumeranno, occorre evidenziare che le strutture sanitarie sono sistemi adattativi complessi (Wright, Hill 2005); ossia, sistemi che si specificano in assetti organizzativi molteplici e interconnessi, che tendono a ridefinire costantemente il rapporto tra sistema e ambiente (centro/periferia, sistema dell'assistenza ospedaliera e delle cure primarie, sistema dei professionisti clinici e dei professionisti convenzionati, strutture accreditate e apparati regionali) dovendo assorbire una crescente domanda di forme assistenziali innovative e ad elevato contenuto tecnologico. In altri termini, si tratta di sistemi che devono rispondere alla complessità con un più alto livello di organizzazione. E', dunque, in quest'ottica che diviene fondamentale la leva del contenimento dei costi che non significa tagli lineari agli investimenti, ma razionalizzazione degli interventi resa possibile dalla conoscenza territoriale/locale dei bisogni e del livello di offerta delle prestazioni e dei servizi (Maino 2009, 96).

In questo quadro di riferimento, la gestione del sistema procedimentale e documentale informatico, rappresenta il prerequisito necessario dell'avvio di un sistema e-health, sostenibile sotto il profilo finanziario e sociale, anche se detta sostenibilità resta tuttavia dipendente anche dall'attività di risk management, un'attività finalizzata al miglioramento continuo della pratica clinica e al monitoraggio del livello di integrazione tra le fasi dei processi.

In Europa, con la Comunicazione del 30 aprile 2004 della Commissione europea dal titolo "*Sanità elettronica: migliorare l'assistenza sanitaria dei cittadini europei*"[4], è stato redatto il Piano di azione della sanità elettronica, ossia, un documento che prevede l'impiego delle Information and Communication Technology (ICTs) per migliorare la qualità dell'assistenza sanitaria in tutti gli stati membri; si tratta in breve, di un impegno propositivo a fornire un insieme di servizi digitali: cartelle cliniche informatiche, ricette mediche, trattamento dei dati, autenticazione dei pazienti, tessere sanitarie, consulenza medica a distanza (teleconsulto), terapia e cura a distanza (telemedicina), oltre che una più rapida installazione di reti internet a banda larga destinate all'interoperabilità dei sistemi sanitari (Weerasinghe 2008; Demiris 2004; Iakovidis, Wilson, Healy 2004).

L'innovazione tecnologica può contribuire al necessario ridisegno strutturale ed organizzativo della rete di assistenza sanitaria, sostenendo lo spostamento del fulcro dell'assistenza sanitaria dall'ospedale al territorio favorendo la continuità assistenziale delle cure e l'integrazione socio-sanitaria, attraverso modelli assistenziali innovativi effettivamente incentrati sul cittadino e sul suo diritto bisogno di salute, allo scopo di migliorarne la qualità di vita, facilitando l'accesso alle prestazioni socio-sanitarie sul territorio nazionale (Ugenti 2010). L'obiettivo è rendere l'e-health una prassi degli operatori sanitari, dei pazienti e dei cittadini, realizzabile, tuttavia, solo attraverso contestualizzazioni che sappiano integrare le azioni locali con le politiche nazionali e comunitarie, in un'ottica di organizzazione dell'apparato pubblico in grado di coinvolgere la

[4] Bruxelles, 30 aprile 2004 COM(2004) 356 definitivo in http://www.europa.eu.int.

dimensione evolutiva del fenomeno burocratico, la tutela del diritto alla salute e l'attuazione del federalismo.

Ciò può avvenire adottando una visione che supera il tradizionale concetto di burocrazia teorizzato da Weber (1922) e che porta all'affermarsi di un nuovo paradigma al quale le amministrazioni pubbliche devono fare riferimento, ossia quello dell'amministrazione digitale (Limone 2008, 19), un paradigma che fissa nuovi criteri di ammissibilità all'indagine scientifica sul processo di riforma degli apparati pubblici (così come delineato a partire dall'emanazione del D.Lgs 39/1993 riguardante le Norme in materia di sistemi informativi automatizzati delle amministrazioni pubbliche, fino all'entrata in vigore del D.Lgs 82/2005, Codice dell'Amministrazione Digitale).

Il percorso evolutivo che serve a tracciare i profili organizzativi degli apparati complessi non può prescindere, dunque, dall'importanza della teorizzazione di Kuhn (1999) secondo cui le rivoluzioni scientifiche si caratterizzano per il passaggio da un paradigma ad un altro; ciò vale anche per le organizzazioni pubbliche le quali sono sottoposte alla dinamica dei paradigmi culturali e in base ai quali, il passaggio da un paradigma (nel quale non si riconoscono più) ad un altro implica l'adozione di nuovi modelli, metodi e prassi (Limone 2008, 17). Oggi, parlare correttamente di amministrazione digitale nella società dell'informazione, ed in particolar modo nell'ambito medico-sanitario, significa verificare preliminarmente il contesto organizzativo più idoneo per gestire i processi di innovazione tecnologica e analizzare le condizioni organizzative quale prerequisito di quelle tecnologiche. Infatti, se il contesto organizzativo non risponde a concreti parametri di efficienza, efficacia, pubblicità ed economicità (censimento e razionalizzazione delle attività cliniche; reingegnerizzazione dei processi; controllo di contabile e di gestione alimentato da un sistema di dati affidabile e certificato; costi ridotti delle attività; sistema informativo e documentale come risorsa fondamentale per la programmazione, la gestione, il governo ed il controllo; sistema procedimentale prevalentemente digitale, efficiente, efficace, economico, rapido, chiaro, semplice e certo nei tempi e nei provvedimenti; adozione del protocollo informatico; servizi in rete; trattamento dei dati; qualità dei servizi all'utenza; risorse umane operanti in un contesto rinnovato per strutture e profili professionali; utilizzo dei mezzi e degli strumenti di comunicazione telematici), anche lo stesso processo di e-health viene messo in discussione, anzi stenta a decollare (Limone, Di Viggiano, Preite 2003).

Tali elementi costitutivi del nuovo paradigma presuppongono, tra l'altro, la necessità di riportare l'attenzione sui processi di riorganizzazione delle strutture e delle funzioni interne (back-office), piuttosto che sulle attività esterne (front-office); l'intervento sistematico sul back-office assicura, infatti, che i processi di automazione siano fondamentali per le attività del front-office (Mancarella 2009), a condizione che le informazioni cliniche, gestionali ed economiche siano validate e rese disponibili in digitale nelle transazioni tra operatori e tra strutture sanitarie, consentendo così l'acquisizione dei dati direttamente al momento della produzione dell'informazione e ottimizzando l'accesso ai dati individuali dei pazienti (Paccaud 2006, 48); solo attraverso l'integrazione digitale tra le applicazioni, i flussi e le procedure cliniche si possono garantire standard elevati di qualità nell'erogazione dei servizi sanitari e nella continuità assistenziale (Fontana 2005).

La disponibilità di dati certi, in grado di rappresentare i diversi aspetti e componenti del sistema, è essenziale altresì per comprendere quale sia la reale situazione, in particolare relativamente ai

risultati prodotti, sia sotto il profilo strettamente sanitario (miglioramento della salute, aumento della sopravvivenza, riduzione della sofferenza, etc.) sia relativamente alla coerenza con il mandato generale (accessibilità, equità) e la sostenibilità (costi, miglioramento dell'efficienza). Da qui, la crescente attenzione circa gli aspetti inerenti la qualità dei servizi che ha comportato una crescita della domanda di informazioni sia in senso quantitativo sia in senso qualitativo, con richiesta di indicatori precisi, affidabili, specifici, aventi valore legale e in grado di rappresentare in modo esauriente i fenomeni oggetto di interesse, permettendo ai responsabili (clinici, gestionali, politici) di prendere le decisioni più appropriate (Liva 2007, 113).

Le funzioni di un sistema e-Health, che sfrutta le ICTs per migliorare le prestazioni e abbassare i costi dei servizi sanitari riguardano: a) l'analisi dei parametri vitali di pazienti, ove possibile, mediante micro apparecchiature gestite con la cooperazione del paziente stesso anche allo scopo eventuale di monitoraggio continuativo; b) la trasmissione dei dati a una stazione di comunicazione locale (in abitazione o ambulatorio) e da questa a database centrali e al personale medico; c) il feedback da parte del personale medico, consistente in pareri, consulti e decisioni su esami, interventi e cure; d) raccolta e trattamento digitale di dati ausiliari alla preparazione di cartelle cliniche e anamnesi; e) coinvolgimento dei pazienti nell'opera di controllo e somministrazione di cure (Vacca 2007).

L'innovazione tecnologia e l'impiego delle ICTs assumono, inoltre, una cruciale importanza in termini di generatore di sviluppo per due principali ordini di motivi:

1. da un lato, vengono considerate generatori di efficienza per il sistema sanitario e di miglioramento dell'offerta complessiva di prestazioni per il paziente, sia attraverso specifiche decisioni di politica sanitaria (es. la promozione al ricorso delle cure domiciliari attraverso modelli alternativi di organizzazione del servizio con dispositivi innovativi di tele-assistenza), sia attraverso nuove procedure assistenziali che si servono di tecnologia innovativa per lo sviluppo di percorsi diagnostici e terapeutici, di particolare efficacia in termini di outcome;
2. dall'altro, vengono considerate fattori di successo per lo sviluppo economico del Paese in quanto generatrici di nuovi impulsi, sia per l'ulteriore sviluppo nel campo della ricerca applicata e della conoscenza, sia per il trasferimento dell'innovazione stessa sul mercato.

In tale contesto, il settore sanitario rappresenta l'ambiente ideale per combinare l'attività di ricerca "sul campo" sia di tipo sperimentale che di tipo industriale, alla creazione di un indotto di imprese ad alto contenuto innovativo per la creazione di moderne tecnologie (bio-mediche e sanitarie) e la produzione di farmaci innovativi. Le nuove conoscenze, frutto di tale combinazione, hanno originato ambiti scientifici quali la genomica, la telemedicina, la bioinformatica, con un forte impatto economico e sociale oltre che sul diritto stesso alla salute (Piano Sanitario Nazionale 2006-2008, 14).

4. La gestione del rischio in sanità

I primi studi sul rischio clinico sono stati avviati a partire dall'esame di eventi conseguenti a trattamento medico dal quale sia derivata disabilità o prolungamento del ricovero ospedaliero (*California Medical Insurance Feasibility Study*, 1974), ma è solo con la pubblicazione del rapporto

To err is human (Institute of Medicine, Washington 2000) che il tema dell'errore umano in medicina si colloca al centro dell'attenzione degli studiosi, dei professionisti e delle istituzioni. Si tratta di una svolta decisiva, che ha alimentato specifici programmi di ricerca, finalizzati ad analizzare il rapporto tra ICTs e gestione del rischio nell'ambito della più generale questione relativa alla qualità e sicurezza dei servizi (Esteves, Joseph 2008). Le ICTs rappresentano, infatti, strumenti efficaci di supporto alla struttura organizzativa e ai processi decisionali (clinical decision support system, health technology assessment), oltre che all'implementazione ed al monitoraggio del rischio (clinical data repository, electronic medical record).

In Italia, i primi progetti significativi sono stati avviati agli inizi del duemila ed hanno riguardato prevalentemente la prevenzione e la gestione del risk management sanitario attuata attraverso la reingegnerizzazione del sistema informativo, la gestione elettronica del flusso delle prescrizioni farmaceutiche, l'introduzione del trattamento digitale delle immagini ed il processo di digitalizzazione del sistema documentale sanitario (Capocelli, Dario 2008).

Si evidenzia, dunque, che il problema del danno al paziente è un rischio generalizzato che coinvolge tutti i Paesi e i rispettivi sistemi sanitari in una presa d'atto dei numerosi cambiamenti in corso sia all'interno dei servizi sanitari, sia nel rapporto tra questi e "l'esterno". Tuttavia, si è in presenza di spinte non sempre convergenti con i rispettivi obiettivi, e insufficienti a determinare reali ed efficaci azioni di miglioramento della sicurezza dei pazienti. Il problema del rischio clinico richiede, infatti, anche un profondo cambiamento culturale di tutti gli attori coinvolti nel processo.

Il presupposto di una corretta gestione del rischio clinico richiede, dunque, un cambio di prospettiva che conduce dal concetto di gestione degli eventi sfavorevoli a quello di gestione del rischio; in altri termini è necessario il passaggio da un sistema esclusivamente reattivo (gestione della non conformità, gestione delle emergenze ecc.) a un sistema prevalentemente pro-attivo e preventivo.

Un ulteriore aspetto è rappresentato dalla necessità che aumenti l'attenzione alla sicurezza dei pazienti con riferimento a tutti i livelli dell'organizzazione. Gli eventi avversi rappresentano, indubbiamente, un problema di qualità delle cure e, in tal senso, hanno un rilievo prettamente clinico, ma presentano anche un risvolto economico-finanziario legato ai costi sostenuti dalla struttura sanitaria e ancora, determinano la perdita di fiducia della popolazione nei confronti del servizio sanitario comportando una lesione del diritto alla salute. La sicurezza dei pazienti, assume in questa prospettiva, una rilevanza che coinvolge tutte le fasi e gli aspetti dell'organizzazione, vincolando l'effettiva applicabilità delle soluzioni individuate, alla capacità di gestire sinergie multidisciplinari (mediche, manageriali ed economiche) e coinvolgimento dei diversi livelli organizzativi. La mancanza di integrazione tra i diversi livelli organizzativi o la predominanza di alcuni su altri, determina la perdita di componenti essenziali della gestione del rischio clinico con la conseguenza di fornire visioni parziali o artificiose. In mancanza di una siffatta integrazione, l'area legale-amministrativa di una determinata struttura sanitaria, che ha l'interesse di prevenire e gestire il contenzioso, risulterà distaccata da quella tecnica, finalizzata ad aspetti tecnologici e strutturali e, ancora da quella clinica, concentrata sull'outcome dei trattamenti sanitari con conseguente perdita della sistematicità che la gestione del rischio richiede. Se è vero che il fine primario di un'azienda sanitaria è la tutela della salute dei pazienti e della popolazione, è anche evidente che le strategie di risk management dovranno focalizzarsi

sulla prevenzione e gestione dei rischi secondo il principio ippocratico del *primum non nocere* (Reason 2004, 25). A ciò, si aggiunge il fatto che è ormai fisiologica, negli ambienti sanitari, la crescita della percentuale su un contenzioso che, tra l'altro, diviene sempre più aspro e visibile tra cittadini e operatori sanitari.

Per quanto riguarda il nostro Paese, non esistono studi epidemiologici specifici che possano dare informazioni sulle dimensioni del fenomeno. Le valutazioni fatte ad oggi si basano, nella maggior parte dei casi, sui dati diffusi dal Tribunale per i Diritti del Malato (Inglese, 2002). In particolare, l'associazione sottolinea come i particolari contatti con il Tribunale per i sospetti errori medici siano notevolmente aumentati negli ultimi anni. Sulla base dei dati forniti dalla stessa associazione è possibile, inoltre, compiere valutazioni e confronti tra aree specialistiche. Più della metà delle segnalazioni sono concentrate in quattro aree: ortopedia, oncologia, ostetricia e ginecologia, chirurgia generale. Questi dati, seppure interessanti dal punto di vista qualitativo, risultano poco utilizzabili per una valutazione quantitativa del problema "rischio clinico". I limiti, in tal senso, di un dato rilevato dalla segnalazione dei pazienti sono evidenti: da un lato è influenzato dalla *compliance* alla segnalazione, che a sua volta dipende da una serie di fattori difficilmente controllabili (spinta dei media, sensibilizzazione a livello locale ecc.) e dall'altro è prevedibile che non vi sia una perfetta corrispondenza tra eventi segnalati ed eventi realmente accaduti, con possibili sovra o sottostime (Novaco, Damen 2004).

La letteratura fornisce numerose definizioni di risk management, ma l'idea unificante è comunque il riferimento alla gestione di tutti i rischi che mettono in pericolo il valore di un'organizzazione, e che coinvolgono i diversi aspetti e le differenti dimensioni del fenomeno organizzativo. Il risk management rappresenta, dunque, un approccio metodologico strutturato, poiché, diretto a valutare rischi che sono già individuati o individuabili come tali; infatti, senza la conoscenza del rischio viene meno la stessa possibilità di adottare azioni correttive o migliorative.

La fase di gestione del rischio in ambito sanitario si traduce sostanzialmente in due fasi:

La prima riguarda l'identificazione dei rischi, o la rilevazione degli eventi sfavorevoli (eventi avversi), considerati precondizioni del rischio stesso. L'identificazione è attuata attraverso le fonti informative che, se digitalizzate, possono rispettare due condizioni:

1. la prima condizione riguarda la semplicità della consultazione, cioè, occorrono fonti informatizzate dalle quali sia possibile trarre informazioni su singoli eventi ed effettuare delle indagini statistiche; rientrano in questa tipologia di flussi informativi la cartella clinica digitale, la scheda digitale di dimissione ospedaliera ed il report digitale dei reclami degli utenti;
2. la seconda condizione riguarda la quantità e l'integrazione delle informazioni sullo stesso caso; per esempio, la scheda nosologica digitale (sulla classificazione sistematica delle malattie), consente di trarre informazioni sul tipo di complicanze di un ricovero, ma consente anche di risalire alla documentazione clinica digitale completa del paziente. Quindi è il tipico esempio di flusso informativo che può essere utilizzato come strumento per la mappatura del rischio e come strumento di *screening* per risalire a eventi avversi specifici.

La fase successiva si sostanzia nel risk assessment, ossia nella gestione e nella valutazione della probabilità e della gravità degli eventi che si possono verificare, con la finalità di eliminare il

rischio, o ridurlo ad un livello accettabile. Tale fase prevede la redazione di una mappatura degli incidenti: il c.d. incident reporting che, unitamente alla revisione della cartella clinica digitale, consente di giungere ad una valutazione quantitativa degli eventi avversi. La costruzione degli incident reporting trova legittimazione nella teoria dell'errore latente, cioè in una prospettiva che evidenzia due fenomeni connessi al rischio: da un lato gli errori umani (definiti dalla letteratura internazionale: slips, lapsus, mistakes), dall'altro le violazioni di norme, regole e protocolli.
Sulla base di queste premesse, Reason ha elaborato un modello finalizzato ad individuare e diagnosticare gli errori in sistemi socio-tecnici complessi. In particolare, il modello consente di evidenziare che il contributo umano alla genesi degli incidenti si colloca a due livelli: latent failure (errore latente) e active failure (errore attivo). Gli errori latenti sono definiti "patogeni", in quanto in grado di dare origine a eventi patologici quando si combinano con altri fattori, venendo meno la natura potenziale degli stessi (Reason 1990). E' evidente, dunque, l'esistenza di un rapporto causa (patologie del sistema) effetto (rischio clinico) che deve favorire l'innesto sinergico della metodologia manageriale nella gestione delle informazioni, dei dati e dell'erogazione di servizi. In altri termini, il concetto cardine di un modello avanzato di e-health è il processo, inteso come ottimizzazione di performance che dipende dall'intera catena di attività interconnesse e non già da attività funzionali separate, ottimizzazione che è resa possibile dalla applicazione delle ICTs a tutto il comparto sanitario. A titolo esemplificativo, si pensi al vantaggio di imputare i dati del paziente una sola volta e in modo che gli stessi risultino accessibili da qualsiasi reparto ma, soprattutto, che risultino protetti e tutelati contro accessi non autorizzati, perdita o diffusione illecita e da possibili errori su: refertazione, terapie, prescrizioni di varia natura e somministrazione di farmaci.

5. La gestione del patrimonio informativo in sanità

Le recenti politiche dell'e-health, impongono una necessaria riorganizzazione delle infrastrutture informatiche da parte dei diversi apparati pubblici (come previsto dal Codice dell'amministrazione digitale), i quali saranno tenuti a "supportare" il flusso dei documenti in formato elettronico, validato giuridicamente mediante apposizione di firma digitale e tecniche di marcatura temporale; inoltre, dovranno prevedere la possibilità di un accesso esterno, opportunamente controllato, ai documenti afferenti ai diversi iter amministrativi, nonché il controllo dello stato di avanzamento di ciascuno di essi. Tale scambio di dati deve poter avvenire sia all'interno della stessa amministrazione, sia tra amministrazione e cittadino, sia fra strutture amministrative diverse, mediante accesso telematico ai sistemi informativi della struttura.
Il sistema documentale delle strutture sanitarie, quindi, dovrà essere definitivamente trasformato in un sistema informativo specializzato e ispirato a criteri uniformi (Guercio 2001)[5], altamente qualificato, con un sistema ICT che preveda:

[5] Cfr. M. Guercio (a cura di), La gestione elettronica dei documenti e la tenuta degli archivi, 2001; ID., Le norme

a. la condivisione delle informazioni (e quindi dei documenti) all'interno del sistema amministrativo e con i cittadini;
b. la riduzione delle operazioni di routine e il miglioramento della qualità dei risultati;
c. l'automazione delle attività di acquisizione e organizzazione dei documenti d'archivio (registrazione, classificazione/fascicolazione dei documenti);
d. lo scambio telematico dei dati di registrazione e l'accesso in rete ai sistemi documentali (compatibilmente con i limiti dettati dalle norme sulla sicurezza e sulla riservatezza dei dati personali), mediante lo sviluppo di regole e di formati che garantiscano l'interoperabilità;
e. la produzione, trasmissione e conservazione di documenti informatici giuridicamente validi, autentici e affidabili, ricorrendo a meccanismi di firma elettronica o digitale;
f. l'integrazione dei flussi di lavoro amministrativo e documentario grazie all'utilizzo di programmi di workflow management e strumenti di telelavoro (gestione dei flussi documentali).

L'attuale sistema informativo sanitario deve essere, dunque, progettato per attestare la storia clinica del paziente o del fascicolo personale e basato su una architettura di "cooperazione applicativa", i cui componenti software devono essere scelti in funzione della qualità e della corrispondenza ai requisiti funzionali richiesti al fine di evitare che la molteplicità dei componenti comprometta una visione unitaria ed organica del sistema informativo. Sotto il profilo qualitativo e sostanziale, deve necessariamente offrire coerenza nelle relazioni interne tra i dati, offrire una visione integrata del contenuto all'utente, risultare affidabile sia nelle tecnologie sia nei dati e consentire la coesistenza di sistemi applicativi diversi, resa indispensabile dalla eterogeneità e complessità degli ambiti interessati.

Il primo passo consiste nell'istaurare un colloquio, veloce e bidirezionale, tra le applicazioni al verificarsi di specifici eventi. A titolo esemplificativo si pensi alla fase di ingresso di un paziente per una determinata visita (prenotata tramite CUP: Centro Unico delle Prenotazioni): le informazioni e i dati informatici identificativi del paziente e dell'attività diagnostica/terapeutica prevista devono essere comunicati al sistema di gestione dell'ambulatorio (applicazione clinica); una volta prodotto il documento di sintesi della visita (referto) questo dovrà transitare per il *Repository* dei dati clinici ove rimarrà a disposizione del medico di base (Toci 2006, 9).

Nell'architettura del sistema informativo delle aziende ospedaliere, il *Repository* dei dati clinici rappresenta il cuore il tutto il sistema, il punto di raccolta strutturata di tutti i dati sul paziente generati dai vari sottosistemi clinici, il collettore dei documenti di sintesi di tutte le attività svolte nel tempo sul paziente. In sintesi, rappresenta uno strumento di comunicazione trasversale sul paziente attraverso l'utilizzo di protocolli comunicativi standard; contiene le regole per il rispetto della normativa sulla privacy ed è utilizzabile mediante strumenti di autentificazione certa (smartcard); è oggetto di autorizzazione da parte del paziente per l'accesso ai dati clinici, da parte del proprio medico o ad altri specialisti esterni autorizzati; è l'unica interfaccia che rende disponibili le informazioni all'intero sistema e consente di visualizzarle, sia come sequenza temporale di eventi clinici (nei singoli documenti), sia raggruppando i documenti

sulla gestione informatica dei documenti in Testo Unico e Autocertificazione: la guida per le amministrazioni, Dipartimento della Funzione Pubblica - Presidenza del Consiglio dei Ministri, 2001

per branca specialistica; contiene , in sintesi, tutto ciò che serve agli altri soggetti che svolgono attività a vario titolo sul paziente. Il *Repository* è, infine, la componente che entra nel sistema regionale di integrazione dei dati sul paziente.
Inoltre, nella gestione delle richieste di prestazioni sanitarie per i pazienti interni, queste possono essere complesse e indirizzare a più reparti diagnostici e terapeutici (laboratorio, radiologia, cardiologia, anatomia patologica); il sistema deve, dunque, consentire all'operatore di fare una richiesta unica per una qualsiasi combinazione di prestazioni. Individuato il percorso che il paziente deve percorrere, è il sistema informativo che, nel suo complesso, si farà carico di suddividere la richiesta in funzione dei vari sottosistemi che, in cascata, gestiranno le singole prestazioni e di inviarle agli stessi. L'immissione è controllata e guidata per garantire la coerenza logica (compatibilità) dell'insieme delle richieste e la loro frequenza. Una volta immesse e smistate le richieste, il sistema di *Order Entry* riceve un feed-back da ogni sottosistema coinvolto. Il feed-back è completato da un'accettazione formale della richiesta con la data di erogazione della prestazione.
L'introduzione di tale metodologia offre dei vantaggi operativi in termini di abbattimento di tempi e di costi e permette di realizzare:

a. *dematerializzazione* delle richieste cartacee (usualmente formalizzate su moduli specifici e molto costosi;
b. *standardizzazione*, con le scelte tabellari della combinazione delle prescrizioni, della semantica delle richieste;
c. *identificazione* univoca del paziente, che risolve i problemi di errata associazione in tutti i sottosistemi;
d. *creazione delle basi informatiche* necessarie per poter consegnare i referti alle varie unità operative con modalità digitale scaricando i dati nel *Repository*.

Tale metodologia rappresenta, dunque, un potente strumento di diffusione culturale di tipo informatico/informativo all'interno della struttura ospedaliera, sia di apprendimento, sia di razionalizzazione dei processi. Definire, infatti, un preciso flusso procedurale e introdurre delle precise regole in fase di caricamento delle richieste permette di rendere lineari i processi all'interno dei servizi diagnostici stessi, aprendo la strada ad una loro ulteriore e successiva informatizzazione in un quadro di sostenibilità finanziaria.

6. L'efficacia degli strumenti dell'e-health: l'Electronic Medical Record

L'electronic medical record (di seguito cartella clinica informatica) è uno strumento indispensabile per lo svolgimento dell'attività sanitaria che ha assunto, nel tempo, una rilevanza essenziale per ogni valutazione giuridica (a fini civili, assicurativi, penali, amministrativi e contabili) delle patologie di una persona e delle responsabilità dei soggetti che le hanno cagionate o che hanno commesso errori diagnostici o terapeutici. Essa è il documento sanitario che attesta la storia clinica del paziente e che adempie alle funzioni di diario del decorso della malattia e di tutti gli altri fatti clinici rilevanti (reperti, visite, diagnosi, terapie, esami ed

interventi) che devono essere annotati contestualmente al loro verificarsi. Il diario clinico deve essere redatto in modo cronologico e deve essere completo di tutti i dati significativi della degenza; inoltre, ogni annotazione è "definitiva", perché, una volta fatta, assume autonomo valore documentale ed efficacia giuridica non appena viene redatta (Fiordalisi 2006, 331). Le modifiche e le integrazioni, dopo che l'atto è stato formato, integrano un falso punibile, anche se il soggetto abbia agito per ristabilire la verità, sono consentite solo correzioni che non danno luogo ad alterazioni delle parti originarie. Secondo la Cassazione, ogni atto esperito sul paziente, sia esso diagnostico o terapeutico, deve esser trascritto in cartella contestualmente alla sua esecuzione ed ogni annotazione, appena è compiuta, esce dalla disponibilità del suo autore e possiede il carattere della "definitività"; quindi i requisiti sostanziali della cartella clinica sono: la veridicità, la completezza, la precisione e la chiarezza delle informazioni riportate (*ivi* 333).

Nel nostro ordinamento giuridico manca una norma sull'intera struttura documentale e sui contenuti indefettibili della cartella clinica informatica, anche un riferimento importante è riconducibile all'insieme delle norme sulla validità giuridica del documento informatico contenute nel Codice dell'amministrazione digitale.

Sotto il profilo tecnologico e organizzativo, come si è avuto modo di anticipare nel paragrafo precedente, la cartella clinica informatica rappresenta un framework applicativo complesso e sofisticato la cui struttura è basata su un database contenente le informazioni cliniche (repository). Le cartelle cliniche elettroniche, inoltre, basano le loro funzioni principali su di un formulario medico (controlled medical vocabulary), un nomenclatore di tutte le possibili prestazioni che consente la comparazione e il confronto dei dati presenti nell'applicazione. Senza un formulario medico di prestazione e di farmaci ben definito, il sistema di supporto decisionale (clinical decision support system) e quello per la gestione dei workflow non potrebbero operare. La struttura di base di una cartella clinica elettronica, in generale, consente a tutto il personale clinico di redigere e rivedere la documentazione, stilare ordini sia di farmaci sia di terapie ed esami e di gestire il prontuario farmaceutico (Friedman, Halpern, Fackler 2008).

L'introduzione di questo efficace strumento dell'e-health, può soltanto migliorare la gestione delle informazioni in termini di velocità, chiarezza, coerenza e accessibilità, di conseguenza la fase iniziale del progetto deve consistere nell'analisi dei processi e nella selezione di quei processi che si vuole migliorare sia nel breve sia nel lungo termine. Soltanto dopo aver ben definito le esigenze organizzative e di conseguenza aver realizzato un dettagliato documento di specifiche tecniche e funzionali, è possibile partire con la fase relativa all'erogazione di servizi. Il modo con cui le informazioni vengono raccolte, immagazzinate, distribuite ed usate comporta notevoli vantaggi sia amministrativi, sia clinici, tra cui:

a. il miglioramento della accessibilità e della disponibilità delle informatizzazioni contenute nella cartella clinica;
b. la diminuzione del tempo impiegato nella digitazione dei dati;
c. la diminuzione dell'incidenza degli errori umani;
d. la diminuzione del tempo impiegato nel realizzare copie della cartella.

Questo sistema, inoltre, permette al personale clinico di visualizzare informazioni sempre aggiornate, migliorando così la coerenza delle terapie con la migliore prassi medica o con

i workflow clinici stabiliti per la particolare patologia, eliminando quanto più possibile le informazioni duplicate.

Conclusioni

La dottrina prevalente (Bruni 2010; Freddi 2009; Pitruzzella 2009; Ardissone 2009) considera la sanità un "banco di prova" per il federalismo italiano, a conferma dell'attenzione politica che la questione richiama. Ma si tratta pur sempre della ricerca di un bilanciamento che si svolge lungo una traiettoria evolutiva molto complessa e che coinvolge assetti organizzativi, nuove modalità di gestione, applicazione di nuove tecnologie e dimensione comunicativo-relazionale nei confronti del cittadino/paziente. E' condivisibile che descrivere un modello ideal-tipico, è cosa differente dal concreto operare di un sistema; in altri termini, ancorchè il diritto alla salute si iscriva nell'alveo dell'inviolabilità e la qualità dei servizi erogati debba rappresentare la discriminante dell'agire sanitario, è pur vero che le azioni possibili restano vincolate alle risorse economiche disponibili e alle capacità organizzative e gestionali dell'Ente. In tal senso, l'equilibrio del sistema e la razionalizzazione della spesa sanitaria, sono fortemente influenzati dalla capacità di implementare processi di innovazione compatibili con le risorse date.
Le leve dell'innovazione sono numerose, ma non richiedono la loro contemporanea attivazione. Si tratta di scomporre un problema in unità semplici a partire dalle quali costruire e una adeguata modellizzazione[6] della complessità. In ambito sanitario, una potente leva di innovazione è rappresentata dalla certezza del dato, quale fattore propedeutico alla gestione delle informazioni personali, cliniche e amministrative. In questa prospettiva si colloca la gestione del patrimonio informativo con tecnologie informatiche e la possibilità di isolare singoli processi per intervenire sulla loro ottimizzazione. L'e-Health è, infatti, il risultato di una organizzazione del sistema documentale informatico, che è in grado di contemperare una elevata interdipendenza di variabili, assicurando ricadute positive in termini di contenimento dei costi di gestione, riduzione del contenzioso, controllo del rischio clinico, aspetto quest'ultimo che deriva dalla possibilità di monitorare eventi negativi sia a livello di singoli processi che a livello di gestione delle informazioni e dei dati delle strutture sanitarie (c.d. patologie del sistema che amplificano la possibilità/probabilità dell'errore medico provocando ricadute dannose sulla salute del paziente e sull'equilibrio economico del sistema sanitario stesso, con conseguenti livelli di responsabilità riconducibili agli operatori e alle strutture sanitarie).
In linea con le Direttive europee, i punti focali dell'ultimo incontro sul tema (*eHealth for Individuals, Society and Economy* , EU eHealth 2009, Prague Declaration), rafforzano le linee programmatiche previste per lo sviluppo della sanità in rete e sostengono iniziative di larga portata già avviate. É il caso del progetto *epSOS* (Smart Open Services for European Patients), avviato nel 2008 e finalizzato alla sperimentazione su scala europea del patient summary e

[6] Col termine modellizzazione si intende quel processo cognitivo che porta alla costruzione di un modello di un processo reale, attraverso l'applicazione dei principi basilari di una teoria. La modellizzazione prevede l'interazione con oggetti reali nelle attività di osservazione e sperimentazione.

della prescrizione elettronica allo scopo di assicurare l'interoperabilità delle soluzioni adottate dagli stati membri.
In Italia, questa importante linea di tendenza è confermata dalle prime esperienze a livello locale con la sottoscrizione di un protocollo di intesa (2008), tra il Ministero della Salute, il Ministero per la Pubblica Amministrazione e l'Innovazione e un consorzio di Regioni: Lombardia (capofila), Friuli Venezia Giulia, Emilia Romagna, Toscana, Molise, Sardegna, Abruzzo, Umbria, Provincia Autonoma di Trento), finalizzato alla "*sperimentazione di un sistema per l'interoperabilità europea e nazionale delle soluzioni di Fascicolo Sanitario Elettronico: componenti Patient Summary ed ePrescription*" (progetto IPSE), che potrebbe rappresentare la chiave di volta del cambiamento organizzativo in ambito sanitario nel prossimo ventennio, oltre che una nuova forma di bilanciamento tra risorse scarse e servizi complessi, ripartendo dal diritto alla salute.

RIFERIMENTI BIBLIOGRAFICI

Borgonovi E. (1992), *Verso il governo regionale della sanità. I rischi un una politica sanitaria senza strategia organizzativa*, in «MECOSAN», 2, pp. 6-12.

Buccoliero L., Caccia C., Nasi G. (2005), *e-Health: percorsi di implementazione dei sistemi informativi in sanità,* Milano, McGraw-Hill.

Capocelli A., Dario C. (2008), *Consuntivi ed evoluzioni del progetto di e-government Telemed-Escape*, in «Iged.it - back office», 1, pp. 57-63.

Caroppo M.S., Turati G. (2007), *I sistemi regionali in Italia. Riflessioni in una prospettiva di lungo periodo*, Milano, Vita e Pensiero.

Cavicchi I. (2005), *Sanità: un libro bianco per discutere*, Bari, Edizioni Dedalo.

Cavicchi I., (2007) *Autonomia e responsabilità: un libro verde per medici e operatori nella sanità pubblica*, Bari, Edizioni Dedalo.

Cocconi M. (1998), *Il diritto alla tutela della salute*, Padova, Cedam

Demiris G. (2004), e-Health: current status and future trends, Amsterdam, IOS Press.

Esteves J., Joseph R. (2008), *A comprehensive framework for the assessment of eGovernment project*, in «Government Information Quarterly», 1, pp. 118-132.

Fiordalisi D. (2006), *La cartella clinica e la responsabilità del medico*, in E. Appendino (et alii), *Responsabilità civile e penale e cartella clinica nell'attività medico chirurgica*, Torino, Giappichelli.

Fontana F. (2005), *Clinical governance: una prospettiva organizzativa e gestionale*, Milano, FrancoAngeli.

France G. (2006), *Federalismi e sanità*, Milano, Giuffrè.

Franco D., Zanardi A. (a cura di) (2003), *I sistemi di welfare tra decentramento regionale e integrazione europea*, Milano, FrancoAngeli.

Freddi G. (2009), Presentazione. *Sanità, politica e società* in «Rivista Italiana di Politiche Pubbliche», 2, pp. 5-7.

Friedman L., Halpern N., Fackler J. (2007), *Implementing an electronic medical record*, in «Critical Care Clinics», 10, pp. 69-76.

Guercio M. (a cura di) (2001), *Le norme sulla gestione informatica dei documenti*, in «Testo Unico e Autocertificazione: la guida per le amministrazioni», Dipartimento della Funzione Pubblica - Presidenza del Consiglio dei Ministri.

Iakovidis I., Wilson P., Healy C. (2004), *e-Health. Current situation and examples of implemented and beneficial e-health application*, Amsterdam, IOS Press.

Kuhn T. (1999), *La struttura delle rivoluzioni scientifiche*, trad. it., Torino, Einaudi.

Limone D.A. (2008), *Rivoluzioni organizzative: la teoria dei paradigmi di Thomas Kuhn*, in «eGov - Cultura e tecnologie per l'innovazione», 1, pp. 17-19.

Liva C. (2007), *La misura dei risultati nell'ambito della rete dei servizi sanitari*, in G.F. Gensini, (*et alii*), *Rapporto sanità 2007*, Bologna, Il Mulino.

Luciani M. (1991), *Salute*, I, *Diritto alla salute - Diritto costituzionale*., in *Enciclopedia giuridica*, XXVII, Roma, Treccani.

Maino F. (2009), *La governance della politica sanitaria in Europa tra decentramento e ri-accentramento: alcuni casi a confronto*, in «Rivista Italiana di Politiche Pubbliche», 2, pp. 93-119.

Mancarella M. (a cura di) (2009), *Profili negoziali e organizzativi dell'amministrazione digitale*, Trento, Tangram Edizioni Scientifiche.

Novaco F., Damen V. (a cura di) (2004), *La gestione del rischio clinico*, Torino, Centro Scientifico Editore.

Paccaud F. (2006), *La pianificazione in sanità pubblica*, in C. Cislaghi (a cura di), *Gli scenari della sanità*, Milano, FrancoAngeli.

Pezzini B. (1998), *Principi costituzionali e politica della sanità: il contributo della giurisprudenza costituzionale alla definizione del diritto sociale alla salute*, in B. Pezzini, C.E. Gallo (a cura di), *Profili attuali del diritto alla salute*, Milano, Giuffrè.

Predabissi S. (2009), *Fonti legislative e ripartizione di competenze*, in C. Miriello (a cura di), *Le aziende sanitarie pubbliche*, Padova, Cedam.

Reason J. (1990), *Human error*, Cambridge, Cambridge University Press.

Reason J. (2004), *Introduzione* in Novaco F., Damen V., (a cura di), *La gestione del rischio clinico*, Torino, Centro Scientifico Editore.

Reviglio F. (2003), Diritto di cittadinanza e risorse da *Il diritto alla salute alle soglie del terzo millennio*, Torino, Giappichelli.

Romeo G. (2009), *Il contenimento della spesa nei servizi sanitari regionali: la razionalizzazione del sistema degli acquisti*, in «Le Regioni», 3-4, pp. 545-580.

Toci A. (2006), *Il nuovo sistema informativo dell'Azienda Ospedaliera di Padova,* in «Iged.it - back office», 4, pp. 9-13.

Toth F. (2009), *Le riforme sanitarie in Europa: tra continuità e cambiamento*, in «Rivista Italiana di Politiche Pubbliche», 2, pp. 69-92.

Vacca R. (2007), *ICT al servizio della sanità in rete*, in G.F. Gensini, (*et alii*), *Rapporto sanità 2007*, Bologna, Il Mulino.

Weber M. (1995), *Economia e società*, Milano, Edizioni di Comunità.

Weerasinghe D. (Ed.) (2008), *Electronic healthcare*, London, Springer.

Wright J., Hill P. (2005), *La governance clinica*, trad. it., Milano, McGraw-Hill.

DOCUMENTI

(1992) *Sentenza 23 luglio 1992*, Corte Costituzionale, in «Giurisprudenza Costituzionale».

(2002) *Spesa sanitaria e Patto di stabilità e crescita* di Peres R., in «L'impatto delle riforme amministrative», Relazioni e materiali per l'analisi dei processi nella PA, CNEL.

(2003) *L'innovazione organizzativa e tecnologica nei comuni* (Progetto pilota), Limone D.A., Di Viggiano P.L., Preite G., Ministro per l'Innovazione e le Tecnologie, Università di Lecce.

(2004) *Comunicazione della Commissione europea*, COM(2004) 356, Bruxelles, 30 aprile 2004.

(2005) *Contesti: opportunità e vincoli*, in Piano Sanitario Nazionale 2006-2008, Roma.

(2010) *La eHealth nei progetti del SSN: il ruolo chiave del Fascicolo Sanitario Elettronico,* Ugenti R., Dir. Gen. del Sistema Informativo - Ministero della Salute, Bologna, 16 gennaio 2010.

Rivista elettronica di Diritto, Economia, Management

N. 1 - 2010 · pp. 213-242

Nuove tecnologie per la prevenzione di errori nelle aziende sanitarie Rfid (radio frequency identifier)

Antonino Buscemi

Abstract: RFId (*Radio Frequency Identifier*): Si tratta di un dispositivo hardware e software costituito da una memoria (*chip*) e da un'antenna (*aerial)*, che possono essere riconosciuti e analizzati da un apposito lettore RFId (transceiver). Nella memoria possono essere inserite notevoli quantità di dati che, possono essere letti tramite l'antenna, da un dispositivo esterno. Una importante innovazione in ambito sanitario, l'identificazione RFId è una tecnologia che consente di identificare oggetti e persone attraverso dei microchip che memorizzano informazioni trasmettendole ad un sistema centralizzato, con radiofrequenza. L'obiettivo principale dell'uso, del sistema RFId in ambito sanitario è l'acquisizione di un maggiore livello di sicurezza nella certezza dell'identificazione del paziente. L'attivazione di progetti che utilizzano il sistema RFId rispetta la normativa vigente sulla privacy. Molti progetti telematici, integrano la tecnologia RFId nelle proprie applicazioni in diversi ambiti: identificazione del paziente nella gestione degli accessi; tracciatura della presenza del paziente nella gestione dei varchi della Struttura; associazione tra paziente e farmaci da somministrare nella gestione delle Terapie. Inoltre, importante sperimentazione deriva dalla rilevazione dei dati corporei (temperatura, pulsazioni cardiache, pressione, ecc.) tramite un sensore posto su di un braccialetto che trasmette i dati con radio frequenza ad un computer portatile. E' quindi possibile ipotizzare appositi progetti di applicazione basati su tale tecnologia, soddisfacendo le esigenze organizzative peculiari delle singole strutture a costi ridottissimi. Inoltre, per la gestione del paziente in reparto, tale programma consente l'organizzazione delle richieste di consulenze specialistiche, di laboratorio, radiologiche ecc., ciò qualifica le modalità di comunicazione tra i reparti ed il servizio, razionalizzando le singole fasi della richiesta e del ritorno dell'informazione al fine di fornire al Reparto idonei strumenti di supporto del processo di assistenza ed organizzativo in tempo reale. Gli obiettivi sono quelli di garantire un corretto scambio informativo tra Reparti e Servizi, di monitorare le richieste di prestazioni eseguite e non, di ricondurre al paziente tutte le prestazioni erogate durante il ricovero. Prevede tutte le fasi di gestione della richiesta, dall'inoltro alla validazione, dalla convalida al sollecito, dalla pianificazione al monitoraggio.

Parole chiave: RFId, Risk Management sanitario, Privacy, Unione Europea, Health;

JEL classification: G3, I0;

Articolo pervenuto il 5 ottobre 2010, approvato il 22 novembre 2010

Sommario: Premessa –Introduzione -1.La sanità come problema sociale -2.La sanità elettronica - 3.Generalità - 4. Il sistema sanitario e le nuove tecnologie per la riduzione del rischio di eventi/errori (il sistema R-FId) - 5. Tecnologia del package intelligente - 6. Tecnologie ottiche - 7. Tecnologie in radiofrequenza - 8. Casi di studio - 9. L'Information Tecnology nella sicurezza trasfusionale - 10. Altre tecnologie - 11.Il sistema Gricode - 12. Implementazione e costi di un sistema Gricode - 13. La terza industria del settore sanitario europeo - Conclusioni

Premessa

La Commissione Europea ha reso noti alcuni dati, inerenti una ricerca commissionata ad un ente terzo, in merito alla sicurezza dei sistemi sanitari. Da questa analisi si evince che: si stima che negli Stati membri dell'Unione una quota compresa tra l'8 % e il 12 % dei pazienti ricoverati presso ospedali subiscono eventi sfavorevoli mentre ricevono assistenza sanitaria[1]. Inoltre, il Centro europeo per la prevenzione e il controllo delle malattie (ECDC) ha stimato che le infezioni associate all'assistenza sanitaria colpiscono in media un paziente ricoverato su venti, ossia 4,1 milioni di pazienti/utenti all'anno nell'UE, e che 37.000 decessi sono provocati ogni anno da infezioni o errori La scarsa sicurezza dei pazienti rappresenta un grave problema per la sanità pubblica ed un elevato onere economico per le scarse risorse sanitarie disponibili. Gli eventi sfavorevoli, sia nel settore ospedaliero che in quello delle cure primarie, sono in larga misura prevenibili e la maggior parte di essi sono riconducibili a fattori sistemici. La Comunità, tramite il settimo programma quadro di ricerca e sviluppo[2], sostiene la ricerca nei sistemi sanitari, segnatamente in relazione alla qualità dell'assistenza sanitaria nell'ambito del tema «Salute», ponendo in particolare l'accento sulla sicurezza dei pazienti. Quest'ultima riceve particolare attenzione anche nell'ambito del tema «Tecnologie dell'informazione e della comunicazione». Lo studio che segue deriva da un esigenza denotata dalle "Raccomandazioni del Consiglio Europeo del 9 giugno 2009" che tra le altre cose invita a sostenere la creazione e l'elaborazione di politiche e programmi nazionali in materia di sicurezza dei pazienti tramite l'inserimento della sicurezza dei pazienti tra i temi prioritari nelle politiche e nei programmi sanitari a livello nazionale, regionale e locale, nonché, il sostegno allo sviluppo di sistemi, procedure e strumenti più sicuri e di facile impiego, compreso l'uso delle tecnologie dell'informazione e della comunicazione.

---

1 Relazione tecnica «Improving Patient Safety in the EU» (Migliorare la sicurezza dei pazienti nell'UE), elaborata per la Commissione europea, pubblicata nel 2008 dalla RAND Corporation;

2 Decisione n. 1982/2006/CE del Parlamento europeo e del Consiglio, del 18 dicembre 2006, concernente il settimo programma quadro della Comunità europea per le attività di ricerca, sviluppo tecnologico e dimostrazione (2007-2013) (GU L 412 del 30.12.2006, pag. 1).gico e dimostrazione (2007-2013) (GU L 412 del 30.12.2006, pag. 1);

Introduzione

Tra le attività dell'Unione Europea[3] è stata presentata una proposta di decisione del parlamento europeo e del consiglio inerente un nuovo programma in materia di salute pubblica per rafforzare la capacità di risposta in relazione alle preoccupazioni dell'opinione pubblica. In tal senso sono state create strette sinergie tra gli Stati membri per sostenere i loro sforzi, onde migliorare la salute della popolazione e l'efficacia dei loro sistemi sanitari; e creando meccanismi sostenibili atti a consentire loro di coordinare le loro attività in campo sanitario. Inoltre, il programma consentirà alla Comunità di far fronte alla sua importante responsabilità di contribuire ad un elevato livello di protezione della salute, come statuito nel trattato. Gli Stati membri spendono un parte importante del loro PIL per la sanità (la media comunitaria si situa ora attorno all'8%).

La spesa per la sanità registra un costante aumento e continuerà ad aumentare anche in futuro, a causa di fattori quali l'invecchiamento della popolazione, lo sviluppo della tecnologia, l'accresciuta domanda da parte del pubblico. In considerazione di ciò, gli Stati membri si adoperano per migliorare i loro sistemi sanitari nell'ottica dell'efficacia dei costi, al fine di affrontare nuove priorità rispettando nel contempo le limitazioni di bilancio. Per poter affrontare tali sfide, essi hanno bisogno di dati ed informazioni migliori e comparabili, ad esempio per quanto concerne la situazione della salute e l'efficacia di particolari interventi in campo sanitario. La Comunità dispone delle potenzialità per sopperire a gran parte di tali esigenze.

Gli sviluppi tecnologici[4] in ambito sanitario saranno oggetto di azioni nell'ambito del nuovo programma. La Commissione intende rafforzare le strutture e i meccanismi di valutazione delle tecnologie sanitarie, incoraggiando la collaborazione tra gli enti interessati, onde perfezionare le metodologie, promuovere le sinergie e contribuire a diffondere in modo efficace i risultati degli studi.

Le nuove tecnologie saranno anche usate per accogliere e diffondere informazioni convalidate. Tra le nuove tecnologie adottate nei sistemi sanitari, nel prosieguo, saranno approfondite quelle che utilizzano per raggiungere il loro scopo le onde radio. In particolare, nell'ultimo decennio i sistemi a radiofrequenza hanno trovato grande applicazione nei sistemi di sicurezza in ambito sanitario in virtù dei risultati connessi alla riduzione degli eventi avversi,e quindi degli errori e del contenzioso, ma anche in esito all'esiguità dei costi della tecnologia utilizzata. Nel nostro studio, l'identificazione tramite RFId sarà punto focale della tecnologia basata su sistemi di radio frequenza in sperimentazione, ma anche in uso in molte realtà del settore sanitario per l'implementazione della sicurezza e per la riduzione del contenzioso e dei costi.

---

[3] Proposta di decisione del Parlamento Europeo e del Consiglio che adotta un programma d'azione comunitario nel campo della sanità pubblica (2001-2006), (presentata dalla Commissione) pag. 10;

[4] Proposta di decisione del Parlamento Europeo e del Consiglio che adotta un programma d'azione comunitario nel campo della sanità pubblica (2001-2006), (presentata dalla Commissione) pag. 18;

1. La sanità come problema sociale

I sistemi sanitari di tutto il mondo si trovano a far fronte a sfide impegnative[5], anche se la natura e l'entità dei problemi da affrontare variano notevolmente tra paesi industrializzati e paesi in via di sviluppo. Le sfide che attendono l'Unione europea sono, in primo luogo, una crescente domanda di servizi sociali e sanitari a causa dell'invecchiamento della popolazione e di livelli di reddito e di istruzione più elevati. Si prevede che nel 2051 quasi il 40% dei cittadini dell'Unione europea supererà l'età di 65 anni[6]; in seconda istanza, le maggiori aspettative degli utenti, che desiderano disporre delle migliori prestazioni constatando al contempo la riduzione nelle disparità di accesso a un'assistenza di qualità, e per ultimo, la crescente mobilità dei pazienti[7] e degli operatori a seguito della progressiva affermazione del mercato interno[8].

2. La sanità elettronica

L'importanza attribuita alla sanità elettronica si iscrive nel contesto più generale del valore aggiunto riconosciuto alle azioni promosse a livello europeo in campo sanitario, che trova riscontro nel programma d'azione comunitario nel campo della sanità pubblica previsto dalla decisione 1786/2002/CE[9]. La Commissione ha inoltre proposto ulteriori misure destinate ad assistere gli Stati membri nel processo di riforma dei sistemi sanitari. Occorrerà monitorare e sottoporre a valutazione comparativa i progressi compiuti e la Commissione ha proposto di applicare il metodo aperto di coordinamento all'assistenza sanitaria e all'assistenza delle persone anziane[10].

Associati ad opportuni cambiamenti organizzativi e allo sviluppo di nuove competenze, i

---

5 COM(2001) 723 def. del 5.12.2001 - *Il futuro dei servizi sanitari e dell'assistenza agli anziani: garantire accessibilità, qualità e sostenibilità finanziaria;* e (6528/03, 20.02.2003). *Sostenere le strategie nazionali per il futuro dell'assistenza sanitaria e dell'assistenza alle persone anziane - relazione congiunta della Commissione e del Consiglio*;

6 Braun, A; A. Constantelou, V. Karounou, A. Ligtoet, & J-C. Burgelman (2003) *Prospecting ehealth in the context of a European Ageing Society: Quantifying and qualifying needs. Final report*. Novembre 2003. IPTS/ESTO: Siviglia, Spagna;

7 Il tema della mobilità dei pazienti forma oggetto di una comunicazione della Commissione, COM(2004) dal titolo *Seguito del processo di riflessione di alto livello sulla mobilità dei pazienti e sugli sviluppi dell'assistenza sanitaria nell'Unione europea*;

8 Il regolamento 1408/71, che coordina i regimi legali di sicurezza sociale, è stato recentemente modificato al fine di semplificare e modernizzare l'accesso all'assistenza sanitaria transfrontaliera, segnatamente nei casi in cui nello Stato membro di origine del paziente si verifichino ritardi ingiustificati. Nel gennaio 2004 la Commissione ha adottato una proposta di direttiva relativa ai servizi nel mercato interno (COM(2004)2 def.) che stabilisce un quadro per la prestazione di servizi nel mercato interno, anche in campo sanitario, e per il rimborso da parte degli enti previdenziali competenti delle cure sanitarie prestate in un altro Stato membro;

9 Decisione n. 1786/2002/CE del Parlamento europeo e del Consiglio, del 23 settembre 2002, che adotta un programma d'azione comunitario nel campo della sanità pubblica (2003-2008), GU L 271 del 9.10.2002;

10 Si veda la relazione di primavera del 2004 - *Promuovere le riforme di Lisbona,* COM(2004) 29 del 21.1.2004. Queste idee saranno sviluppate dalla Commissione in una relazione relativa al metodo aperto di coordinamento nel settore dell'assistenza sanitaria nel 2004. Si tratta di un metodo volto ad aiutare gli Stati membri a sviluppare progressivamente politiche proprie attraverso la definizione di orientamenti e di indicatori quantitativi e qualitativi, la trasposizione degli orientamenti europei in politiche nazionali e regionali e la sorveglianza, la valutazione e la revisione tra pari – cfr. Consiglio europeo, 2000. *Conclusioni della presidenza.* Consiglio europeo di Lisbona, 23-24 marzo, 2000;

sistemi e i servizi della sanità elettronica costituiscono strumenti essenziali di progresso. Essi possono migliorare in modo significativo l'accesso alle cure, la qualità dell'assistenza, l'efficienza e la produttività[11] del settore sanitario. In una recente indagine su vasta scala vengono identificati i differenti approcci adottati dai sistemi e dalle imprese degli Stati membri per trasformare gli aspetti di "*e*Business" della sanità elettronica in fattori determinanti di cambiamento e di crescita della produttività in ambiti quali lo sviluppo delle infrastrutture e delle competenze, i processi aziendali interni, le procedure di appalto e la gestione della catena di approvvigionamento, la commercializzazione e la vendita e le funzioni dell'impresa allargata[12]. L'80% dei costi del settore sanitario, in quanto servizio del settore pubblico, è rappresentato dalle risorse umane e, sia nei vecchi che nei nuovi Statimembri, il 75% della spesa complessiva proviene da fonti pubbliche di finanziamento. La quantità e la complessità delle informazioni e delle conoscenze in campo sanitario sono aumentate al punto tale che la loro elaborazione rappresenta una funzione essenziale di qualsiasi struttura sanitaria. Quello della salute è un settore che fa ampio ricorso alle informazioni e che dipende quindi in misura crescente dalle tecnologie dell'informazione e della comunicazione. È innegabile il contributo offerto da tali tecnologie alla ricerca medica, ad una migliore gestione e diffusione delle conoscenze e all'affermazione di una medicina basata su prove di efficacia. I mezzi offerti dalla sanità elettronica agevolano l'aggregazione, l'analisi e la memorizzazione di dati clinici in tutte le loro forme: gli strumenti di informazione consentono di accedere ai risultati più recenti, mentre gli strumenti di comunicazione rendono possibile una diffusa collaborazione tra organismi e professionisti del settore sanitario.

3. Generalità

L'acronimo RFId indica una tecnologia di comunicazione senza fili che utilizza le onde radio per l'acquisizione di informazioni allo scopo di permettere un corretto salvataggio di dati o di monitorare oggetti e persone.
Fin dal 1895 Marconi realizzò quella che è considerata la prima comunicazione radio a distanza che permetteva sostanzialmente di fare a meno di un collegamento fisico (cavo) tra trasmettitore e ricevente. Verso la fine degli anni '30 comparve il RADAR, che permetteva il rilevamento a distanza di navi e aerei. La tecnologia RFID può essere vista come una combinazione di queste tecnologie. Infatti con la seconda guerra mondiale in Inghilterra fu sviluppato il sistema IFF (Identification Friend or Foe) che montato sugli aerei alleati ne permetteva il riconoscimento distinguendoli da quelli nemici.

---

[11] I sistemi e i servizi della sanità elettronica possono contribuire a ridurre i costi e ad aumentare la produttività nei seguenti contesti i) fatturazione e registrazione, ii) riduzione degli errori medici, iii) riduzione delle prestazioni non necessarie, e iv) risparmi realizzati grazie al commercio elettronico interaziendale, citato da P.M. Danzon e M. Furukawa, e-Health: Effects of the Internet on Competition and Productivity in Health Care (2001) in *The Economic Payoff from the Internet Revolution*, the Brookings Task Force on the Internet, Brookings Institution Press: Washington;

[12] Stroetmann K.A. e V.N. Stroetmann (2004) *Electronic business in the health and social services sector – Sector impact Study No. 10-I (draft). The European e-business W@tch 2003/4*, Commissione europea, Direzione generale Imprese: Bruxelles/ Bonn, febbraio 2004;

Negli ultimi anni, la continua evoluzione tecnologica e la rivoluzione informatica, hanno contribuito ad abbassare drasticamente i costi dei sistemi con conseguente aumento dell'interesse dell'industria nei confronti della tecnologia RFId.

1.1 Componenti del sistema

Un sistema RFID è composto da tre parti:

- **Etichetta (tag)**
  Un trasponder (trasmitter-responder) a radiofrequenza costituito da un circuito integrato con funzioni di controllo dotato di memoria, connesso ad un'antenna, che può essere incorporato in etichette di carta, o contenitori, o anche integrato in apparecchi elettronici come i telefoni cellulari. L'etichetta permette così una trasmissione a corto raggio dei dati memorizzati al suo interno senza la necessità di una connessione fisica;
- **Lettore (reader)**
  Un ricetrasmettitore collegato ad un microprocessore, in grado di "interrogare" il trasponder e ricevere le informazioni da esso inviate;
- **Sistema di gestione**
  Connesso in rete con i lettori, ha la funzione di ricavare, partendo dai dati contenuti nell'etichetta RFId, tutte le informazioni relative agli oggetti e di gestirle in base agli scopi delle applicazioni.

4. Il sistema sanitario e le nuove tecnologie per la riduzione del rischio di eventi/errori (il sistema R-FId[13])

In ambito sanitario sono molteplici le soluzioni tecnologiche che rispondono all'esigenza di una maggiore sicurezza dell'utente/paziente. L'uso di nuove tecnologie per la prevenzione degli errori e la riduzione dei rischi, ancora oggi, non è visto come un tema prioritario. Le prospettive di inserire in ambito sanitario delle innovazione di tale portata, ancora, non sono molte, anche se esistono delle strutture ospedaliere che hanno attivato dei progetti pilota con la collaborazione di alcune aziende che si occupano di tecnologie sanitarie. I sistemi che analizzeremo brevemente di seguito sono un elemento di supporto non indifferente per la sicurezza degli operatori del settore. Tali sistemi ridurrebbero anche lo stress conseguente ad operazioni routinarie, più volte denunciato in letteratura come causa primaria di errori. In un sistema sanitario moderno ed attuale sarebbe opportuno sostituire, dove possibile, i processi manuali, inadatti ad operazioni cicliche ed introdurre invece sistemi computerizzati e automatizzati, in modo particolare in operazioni a rischio, come quelle connesse con l'identificazione del paziente, la somministrazione di un farmaco, prelievo di campioni da analizzare.

Un punto centrale nella reingegnerizzazione del sistema sanitario è rappresentato, infatti, dall'esigenza di considerare l'organizzazione sanitaria come un sistema complesso all'interno

[13] Buscemi A., *Diritto sanitario moderno* 2009, 4, 177-178;

del quale ad alcuni "processi" possono essere applicate le tecnologie più moderne, già introdotte da decenni in altri settori (ad es. lettura attraverso il codice a barre di prodotti di largo consumo), che rendendo disponibili una serie di informazioni in tempo reale potrebbero evitare il manifestarsi di eventi spiacevoli, che non arrecano un danno all'utente, ma sminuiscono la grande professionalità degli operatori sanitari banalmente. Tra le applicazioni che hanno certamente migliorato la sicurezza del paziente c'è l'introduzione di codici a barre per l'identificazione del paziente o dei farmaci.

Sistemi di identificazione di questo tipo, possono contenere un numero molto elevato di informazioni di tipo sanitario che si ritengono particolarmente importanti per il paziente (malattie pregresse, allergie a farmaci, ecc.). Il problema a volte è quello di rendere facilmente accessibili e fruibili, all'operatore, le informazioni.

Come quasi tutti i settori commerciali e dei servizi della società contemporanea, anche la sanità sta andando incontro ad una crescente customizzazione di massa. La tendenza è quella cioè di produrre beni e/o servizi affidabili ed allo stesso tempo in grado di rispondere alle esigenze personali di ogni singolo utente. Mentre in molti altri settori l'utilizzo di sistemi tecnologici, e in particolare ICT (Information and Communication Technology) e robotica, è largamente diffuso, in quello sanitario è per il momento limitato a pochi centri, anche se l'obiettivo è quello di aumentare la sicurezza dei pazienti ed operatori.

I vantaggi dell'applicazione di tecnologie informatiche per aumentare la sicurezza negli ospedali, sono esaminati in un recente studio[14] ed in particolare rispetto a tre aree di sicurezza per il paziente:

1. prevenzione degli eventi avversi;
2. capacità di fornire feed-back rapidi in caso di eventi avversi;
3. possibilità di mappare e comprendere gli eventi avversi.

L'introduzione di sistemi di gestione efficienti permette anche vantaggi economici. Un recente studio, pubblicato sul "American Journal of Medicine" nell' Aprile 2003, ritiene che un sistema di archiviazione dei dati clinici elettronici, possa far guadagnare, in spese evitate ed incremento di reddito, in media ad ogni struttura nell'arco di cinque anni 86,400 dollari, de quali la maggior parte derivante dai costi evitati per la somministrazione di farmaci inutili, seguiti da migliore utilizzo dei test radiologici e da un'efficiente contabilità.

Gli elementi su cui un sistema tecnologico può intervenire per raggiungere questi obiettivi sono diversi e in particolare l'ITC può migliorare la comunicazione tra gli operatori, la cui inefficienza è causa della maggior parte degli errori in ospedale, rendere disponibili informazioni chiave al momento giusto e quindi essere di supporto alle decisioni cliniche.

Un altro importante effetto dell'introduzione di nuovi sistemi tecnologici interattivi consiste nel fatto di riuscire a porre in essere le c.d. "forcing function" o azioni che forzano il sistema, le informazioni prodotte da questo automatismo sono importanti e fondamentali per arginare fenomeni di distrazione dovuti a stress o carichi eccessivi di lavoro.

Infatti, questi sistemi forzano e guidano l'operatore ad eseguire le attività con modalità prestabilite e non danno la possibilità di interpretazioni autonome dell'evento da porre

---

[14] Bates DW, Gawande A.A. *Patient safety: Improving safety with information technology. New England Journal of Medicine*. 2003; 348:2526-34;

in essere o di saltare passaggi operativi; questo metodo può evidenziare automaticamente all'occorrenza, anche possibili errori e situazioni a rischio (allergie da farmaco, interazioni tra farmaci ecc.).

Per esplicitare empiricamente questi sistemi, possiamo dire, che il sistema ha in memoria dei protocolli pre-generati in modo sistemico e rigido che non possono essere aggirati dagli operatori sanitari.

Il successo di sistemi basati sull'utilizzo di ITC e robotica in sanità, è legato alla relativa rigidità dei sistemi proposti e alla difficoltà di utilizzare un unico sistema per integrare diverse funzioni necessarie alla corretta organizzazione dei reparti e alla interazione tra attività strettamente sanitaria e i connessi servizi. Una tecnologia, messa a punto recentemente a livello prototipale per una visione integrata della sicurezza del paziente, è quella proposta dall'istituto Scientifico San Raffaele di Milano, denominata Sistema Ospedaliero Intelligente (SOI)[15].

Questa tecnologia consiste essenzialmente nel seguente insieme di tools coerenti con l'obbiettivo:

1. dotazione al paziente, al momento dell'ammissione, di un braccialetto provvisto di codice bidimensionale (in futuro eventualmente sostituibile con microchip a radiofrequenza che riesce a monitorare la temperatura, la frequenza cardiaca e la pressione) che contiene oltre ai dati anagrafici, anche una serie di informazioni cliniche rilevanti per la sicurezza del paziente (es. allergie a farmaci);
2. Un "carrello intelligente" costituito da un carrello di reparto reso "intelligente" mediante l'integrazione nello stesso di un PC dotato di appositi software utilizzati in varie funzioni, come la catena del farmaco e le analisi di laboratorio, ed inoltre dotato di cassettiere robotizzate per l'erogazione automatica di farmaci destinati ad un determinato utente/paziente, nonché di contenitori per provette di laboratorio, etichette e di un etichettatore automatico. Perché un operatore possa usare il carrello deve farsi riconoscere mediante una personal card che dimostri l'idoneità dell'operatore stesso alla funzione che si appresta a svolgere e ne tracci le attività prestate nel tempo. Poi vi è l'armadio "intelligente" di reparto che agisce da contenitore dei farmaci ed è capace di caricare automaticamente il carrello stesso al termine della somministrazione dei farmaci.

Mediante l'utilizzo di questa tecnologia, l'identificazione del paziente avviene in modo automatico tutte le volte che si debbono eseguire delle azioni sul paziente stesso e, in modo particolare, le prescrizioni di farmaci, l'erogazione degli stessi e cosi anche la preparazione delle provette identificate per l'analisi di laboratorio.

Il sistema è costruito in maniera tale da identificare automaticamente sia l'operatore (tracciabilità-responsabilità dell'operatore), sia il paziente (lettura del braccialetto), sia farmaci da erogare o altro tool da utilizzare per il paziente.

La prescrizione e soprattutto l'erogazione di un farmaco sono effettuate in modo automatico mediante lettura del braccialetto, lettura che da luogo all'apertura automatica del cassetto nella quale sono contenuti i farmaci per quel paziente, in quella dose, al tempo giusto per la somministrazione. Il sistema dà luogo anche a segnalazioni di allarme quando si tenti di

---

[15] Buscemi A., *Diritto sanitario moderno* 2009, 4, 179-180;

somministrare un farmaco al quale il paziente è allergico o non sia stato prescritto o disposta la somministrazione preventivamente
Analogamente, lo stesso sistema è utilizzabile per ottenere all'atto del prelievo ematico, o di altro prelievo, l'esatta identificazione delle provette, azzerando la possibilità di errori.
Questa operazione viene "attivata" dalla lettura tramite penna ottica del braccialetto identificativo, lettura seguita automaticamente dall'erogatore di provette con l'identificazione derivante dal braccialetto stesso.
È in corso di sviluppo l'applicazione sul sistema anche di tecnologie per la rilevazione dei parametri vitali o per esami di POC (Point of Care) come eroga analisi ed altro; in tal modo il futuro fa presagire che sarà possibile eseguire automaticamente ogni tipo di test prescritto all'utente/paziente con evidente riduzione di errori rispetto al codice a barre identificativo, al tipo di analisi da effettuare, al posto letto, all'ora indicata in cartella clinica/infermieristica, e di ottenere automaticamente la registrazione del risultato sul sistema informatico ospedaliero visibile a tutti gli operatori autorizzati.

5. Tecnologia del package intelligente[16]

Una corretta gestione del paziente, orientata alla sua sicurezza, deve prevedere, tra l'altro, sistemi che garantiscono il corretto utilizzo di informazioni critiche per la sicurezza del paziente stesso.
Deve inoltre consentire di utilizzare in maniera facile ed efficiente tali informazioni, facilitando il processo di cura.
Il problema ha dunque differenti step:

- individuazione dei dati utili;
- individuazione delle tecnologie adatte a rendere fruibili tali dati;
- implementazione di tale tecnologie nel contesto del processo di cura.

Preliminarmente analizziamo quali sono i dati di interesse:

- lotto di produzione: la sua identificazione e tracciabilità permette di poter individuare un farmaco in base al produttore, periodo di produzione, materie prime utilizzate, processi di lavorazione adottati;
- consente le seguenti possibili applicazioni: ritiro di tutti i lotti rivelatisi non conformi, o addirittura nocivi, rintracciabilità dei pazienti che abbiano assunto prodotti appartenenti ai lotti da ritirarsi, possibilità di sottoporre a controllo tali pazienti onde evitare conseguenze più serie;
- Data di scadenza: è importante poiché costituisce informazioni basilari sulla validità e sull'efficacia del prodotto;
- ID prodotto: consente di identificare univocamente il tipo di prodotto contenuto all'interno della confezione;

[16] Buscemi A., *Diritto sanitario moderno* 2009, 4, 180;

- ID confezione: è un numero unico e irripetibile che consente di distinguere la confezione da qualsiasi altra;
- Possibili applicazioni: per le indicazioni alle autorità giudiziarie per l'anti-contraffazione, la tracciabilità, l'anti-manomissione.

Le informazioni di cui sopra, e le possibilità applicative che consentono, non sono indipendenti dalla tecnologia adottata per la loro gestione e acquisizione.
Nel seguito saranno trattate brevemente le principali tipologie tecnologiche, cercando di evidenziarne i vantaggi e i possibili svantaggi.

6. Tecnologie ottiche

Si basano sulla lettura automatica, per via ottica, di particolari codici che contengono le informazioni di interesse[17].

Vantaggi delle tecnologie ottiche
- Ampia diffusione;
- Disponibilità di standard
- Basso costo;
- Facile implementazione.

Svantaggi delle tecnologie ottiche
- Lettura singola, codice per codice;
- Relativamente elevata frequenza di non – letture;
- Scarsa capacità di immagazzinamento di informazioni;
- Necessità di orientare il codice in modo opportuno perché possa essere letto.

7. Tecnologie in radiofrequenza

TAG RF-ID: è costituito da un circuito passivo che, irradiato da un antenna emettitrice di onde in radiofrequenza, "risponde" con le informazioni in esso immagazzinate.
La **tecnologia R-FId**[18] (acronimo di Radio Frequency IDentification) ha fatto la sua comparsa, come molte tecnologie di telecomunicazioni, durante la seconda guerra mondiale. Finita la guerra il progredire dei processi tecnologici e produttivi, ha consentito una riduzione delle dimensioni e dei costi. Tutto ciò ha portato questi dispositivi a diventare uno strumento ormai indispensabile in ambito industriale e non. Tra le varie applicazioni basti pensare alla logistica di magazzino, ai sistemi di sorveglianza merci nei supermercati, ai sistemi di accesso in ambienti protetti, fino al pagamento autostradale. Non tutti sanno, infatti, che il telepass, ad esempio, è un'applicazione con tecnologia RFId.

---

17 Buscemi A., *Diritto sanitario moderno* 2009, 4, 181;

18 Buscemi A., *Diritto sanitario moderno* 2009, 4, 181-182;

Negli ambienti **sanitari**, invece, la diffusione di tecnologie wireless ha avuto un lento sviluppo a causa dal pericolo di interferenze con apparecchiature diagnostiche e di monitoraggio. Oggi, tuttavia, lo sviluppo di sistemi di modulazione che consentono trasmissioni efficienti con una bassa potenza di emissione, permette il superamento di questi ostacoli e ha quindi aperto le porte dei luoghi di cura a questa tecnologia. Alcune delle applicazioni più diffuse in campo sanitario, che si stanno attualmente sperimentando in diverse parti del mondo, sono la cartella clinica elettronica, la telemedicina, la gestione della terapia e del farmaco, la localizzazione del paziente all'interno della struttura, la tracciabilità delle sacche di sangue, le applicazioni di supporto all'attività degli infermieri in generale e il controllo della corretta sterilizzazione e manipolazione dei vari strumenti in sala operatoria.
In particolare per questo tipo di applicazione sussisteva anche il problema della resistenza delle applicazioni RFId all'acqua e ai processi di sterilizzazione in genere. Ma anche questo sembra essere risolto. È stato creato, infatti, un TAG che può essere sterilizzato senza bisogno di rimozione e capace di mantenere comunque tutte le proprie informazioni. È stato appositamente pensato per tracciare ogni particolare tipo di apparecchiatura sanitaria che necessita di una pulizia radicale, e può essere programmato per lanciare l'allarme nel caso di compromissione di una qualsiasi fase del protocollo.
L'elemento che caratterizza un sistema RFId è il **transponder** o TAG. Si tratta di un componente elettronico, che può essere largo pochi centimetri e spesso solo pochi millimetri, dove vengono memorizzati i dati di identificazione, questa tecnologia si occupa del controllo e della ricezione/trasmissione dei dati. In particolare ogni TAG ha un identificativo unico dato dal produttore e non modificabile. Il transponder può essere alimentato anche attraverso il campo elettromagnetico prodotto a distanza da un lettore e ricevuto attraverso un'antenna collegata al TAG: in questo caso si parla di **TAG passivi**.
Per accedere alle informazioni contenute nell'etichetta radio è necessario un lettore, che nel caso di RFId passivi ha il compito anche di alimentare l'etichetta. Il vantaggio offerto da questo tipo di tecnologia rispetto ai sistemi di identificazione più utilizzati come i codici a barre, è che il lettore non ha bisogno di avere la visibilità ottica rispetto all'etichetta. Vi è anche un altro notevole vantaggio rispetto ai metodi di identificazione tradizionali. Attualmente è possibile inserire all'interno del TAG, delle memorie non volatili di qualche kilobyte, che possono contenere non poche informazioni. Inoltre, è possibile realizzare RFId che non si limitano a trasmettere informazioni, ma consentono anche di riceverne e aggiornare i propri dati. In questo caso, l'etichetta radio diventa un sistema di identificazione che può tenere traccia della storia di un prodotto durante tutta la sua vita.

8. Casi di studio

In numerose strutture sanitarie si sta sperimentando questa tecnologia. In particolare presso l'**Ospedale Luigi Sacco**[19] di Milano si sta portando avanti la sperimentazione per quanto riguarda le cure domiciliari a malati terminali, prestate in genere da strutture di volontariato

[19] Buscemi A., *Diritto sanitario moderno* 2009, 4, 183-184;

non direttamente riconducibili all'ospedale. È importante, in questo caso, controllare la correttezza della loro erogazione e l'identità delle persone che operano. Ciò si realizza grazie a un TAG RFId posizionato sulla cartella clinica di cui ogni paziente è dotato. Sempre in questo ospedale è stata utilizzata la tecnologia RFId per il controllo della manutenzione delle apparecchiature elettromedicali mentre è allo studio l'utilizzo dei TAG per la tracciabilità del processo delle trasfusioni e per la gestione degli accessi nei laboratori.

Il progetto sviluppato presso il Servizio di Immunoematologia e Medicina Trasfusionale dell'**Ospedale San Raffaele** di Milano è mirato invece alla riduzione del rischio clinico legato al processo di autotrasfusione. Il progetto prevede una fase iniziale di sperimentazione sui processi di autotrasfusione per identificare il sangue prelevato ai pazienti prima degli interventi chirurgici e destinato ad essere trasfuso ai pazienti stessi in caso di necessità nel corso dell'operazione o nel periodo post operatorio. Al fine di correlare le sacche di sangue ai rispettivi pazienti, prima del prelievo viene applicato al polso del paziente un transponder Radio Frequency, che contiene i suoi dati identificativi personali crittografati con sistema di crittografia asimmetrica e una sua foto, e, dopo il prelievo, vengono applicate delle etichette identificative (TAG) alle sacche.

Anche il progetto **Tracciabilità trasfusionale con RFId** è nato con l'obiettivo di gestire il processo trasfusionale. Il progetto è un esempio concreto di successo di applicazione della tecnologia RFId in ambito sanitario, per il controllo e il monitoraggio della filiera trasfusionale ed è stato testato presso il Reparto Trapianto Midollo Osseo (TMO) della Fondazione IRCCS Istituto Nazionale dei Tumori di Milano. Il progetto ha avuto come obiettivo di partenza una maggiore efficienza ed affidabilità nella tracciabilità della filiera trasfusionale, dalla selezione della sacca di sangue fino alla conclusione della trasfusione stessa, contribuendo così a migliorare la sicurezza clinica del paziente. In particolare sono stati reingegnerizzati il processo trasfusionale e gli scambi informativi tra i vari attori coinvolti.

La soluzione adottata consente oggi di identificare in modo univoco sia il paziente, tramite l'adozione di un **braccialetto RFId**, sia ogni sacca, grazie all'applicazione di etichette RFId. L'utilizzo di palmari permette, inoltre, di verificare i dati anagrafici e accedere a informazioni dettagliate di supporto alle decisioni del personale medico, garantendo maggiore tempestività di intervento e congruenza con i dati rilevati. Alla luce dell'esperienza maturata e del riscontro positivo ottenuto in questa realtà, il management della Fondazione IRCCS Istituto Nazionale dei Tumori di Milano ha previsto l'ampliamento del progetto anche verso l'etichettatura delle provette per i prelievi di campioni ematici, nonché l'estensione dell'esperienza acquisita anche ad altri campi applicativi come la tracciabilità informatizzata di farmaci oncologici e reperti di anatomia patologica.

In tutti i casi precedenti si tratta però, di ambiti ben specifici nei quali la tecnologia RFId viene adoperata per affrontare un aspetto particolare della pratica clinica. L'esperienza dell'**ISMETT** (Istituto Mediterraneo per i Trapianti e Terapie ad Alta Specializzazione) di Palermo è, invece, incentrata sulla tracciabilità della gestione del paziente e dei suoi dati clinici, un'attività critica che interagisce in maniera trasversale con i processi controllati dal sistema di gestione della struttura, sia se questo si basi sulle classiche registrazioni cartacee, sia se è presente una gestione totalmente informatizzata, sia se ci si riferisce ad una situazione di tipo ibrido.

I risultati certamente positivi che queste sperimentazioni stanno portando, serviranno a creare una solida base di conoscenze che permetterà nei prossimi anni una diffusione di questa tecnologia negli ambienti sanitari, con tutta una serie di vantaggi di cui il più importante sarà certamente la **riduzione** drastica del numero di incidenti dovuti a scambi accidentali di cartelle cliniche, di farmaci o di sacche di sangue.

8. L'Information Tecnology nella sicurezza trasfusionale (sistemi RFId)

L'implementazione della tecnologia informatica mediante codici a barre o *microchip*, tendente ad una corretta identificazione del paziente, non è rivolta solo ad evitare terapie errate con emocomponenti o con altri farmaci, ma anche l'errata attribuzione dei risultati degli esami di laboratorio. Stanno così nascendo sistemi che hanno lo scopo di evitare un'errata identificazione del paziente sia al momento del prelievo dei campioni di sangue per le analisi, sia al momento della somministrazione di trasfusioni o di farmaci (per es. chemioterapici).
I provvedimenti adottabili, in campo trasfusionale, sono di diverso tipo ed a diversi livelli:

- controllo del gruppo del paziente *bedside* e suo confronto con quello del sangue da trasfondere;
- adozione di braccialetti identificativi;
- adozione di sistemi "a barriera".

Il problema della sicurezza nelle procedure in uso nei reparti delle Aziende Ospedaliere è ovviamente di grande attualità, sia a livello nazionale che mondiale. Da ricordare a questo punto la stessa Raccomandazione n. 5, marzo 2007 del Ministero della Salute per la prevenzione della reazione trasfusionale da incompatibilità AB0, "Nuove tecnologie per ridurre il rischio di errore trasfusionale": "L'implementazione di sistemi di sicurezza, quali **barcode** basati sull'utilizzo di braccialetti identificativi, moduli di richiesta, provette ed etichette dotati di un codice identificativo univoco per ogni paziente o sistemi di identificazione a Radio Frequenza (transponder RFId), possono aiutare ad intercettare errori commessi al momento del prelievo dei campioni o al letto del paziente al momento dell'inizio della trasfusione".
Si vive un presente nel quale si tende sempre di più a cercare di identificare e utilizzare tecnologie di ultima generazione che, in supporto ed aggiunta alle procedure esistenti, garantiscano un maggior controllo volto ad evitare un sempre possibile errore umano.
Come sottolineato dal Ministero una tecnologia, già ampiamente utilizzata in altri settori, che appare particolarmente promettente in tal senso è l'identificazione RFId ad alta frequenza (13,56 MHz, standard ISO 14443 e ISO 15693).
La tecnologia RFId (Radio Frequency Identification) si basa sull'uso dei *Transponder* (TRANSmitter- resPONDER). Il Transponder (detto anche Tag) è un dispositivo elettronico composto di due parti principali: **antenna** e **microchip** (figura 1).
Il microchip contiene anche una memoria non volatile il cui contenuto può essere modificato mediante un lettore-scrittore, noto generalmente con la voce "lettore di transponder".

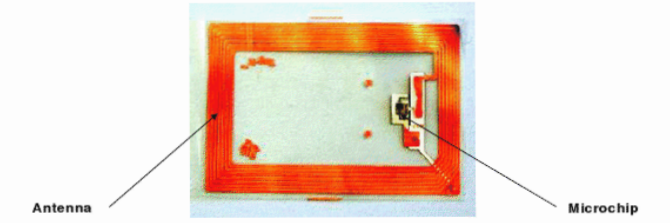
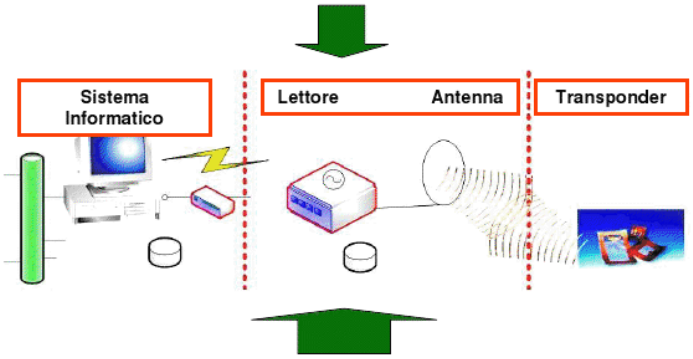


Figura 1: Antenna e microchip

Un lettore di transponder è un dispositivo elettronico che mediante un'antenna comunica con il transponder per rilevare la sua presenza e per eventualmente modificare il contenuto della sua memoria.



I lettori di transponder generalmente non lavorano da soli, ma sono collegati ad un sistema informatico che processa i dati scambiati fra essi e i transponder. Identificazione mediante relativi transponder di ogni unità trasfusionale col paziente a cui è destinata (Figura):

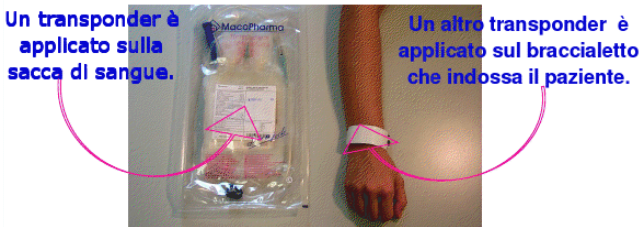


Figura 2: Transponder

Il programma esegue una procedura che abbina elettronicamente e in modo univoco e irreversibile entrambi i transponder, in pratica, i loro chip diventano definitivamente legati uno con l'altro così che una volta abbinati non risulta possibile con nessun metodo alterare lo stato acquisito; esiste anche un metodo di abbinamento elettronico multiplo: un braccialetto può abbinarsi a tante sacche.

I palmari, i computer desktop o laptop dotati di antenna RFId, al momento dell'accettazione verificano il nominativo del paziente prelevando i dati dall'anagrafica del sistema informativo centrale.

A questo punto il professionista consegna un braccialetto, procedendo all'inizializzazione

del tag passivo: il paziente può così essere riconosciuto in modo certo. Sempre tramite un computer palmare o di altro genere, medici e operatori sanitari trasferiscono e prelevano le informazioni grazie ad apposite etichette RFId applicate su ogni sacca al momento della sua assegnazione. Ricevuta la sacca, il professionista deve avere l'unica accortezza di caricare i dati sul sistema informatizzato e, quindi, registrare l'ora di arrivo e leggendo il braccialetto del paziente, eseguire un match dei dati per verificare che la sacca della trasfusione sia quella corrispondente al soggetto. Un'altra operazione di estrema semplicità, ma fondamentale, consiste nell'identificazione tramite badge del professionista che opera la trasfusione. Tale circostanza permette di registrare non soltanto l'ora di inizio ma anche quella di chiusura del processo e comunque raccoglie un insieme di informazioni utili nel contesto.
Grazie alla nuova soluzione offerta dai sistemi RFId la trasfusione si svolge in assoluta sicurezza: nel caso di un'incongruenza dei dati rilevati sul tag della sacca rispetto al braccialetto del paziente, il sistema dà immediata segnalazione visiva e acustica, e non permette di procedere con l'applicazione.
Il sistema informatico consente così al processo trasfusionale di essere sempre trasparente ed affidabile.
La tecnologia applicata al trasfusionale può essere applicata anche nei seguenti ambiti sanitari:

- gestione emocomponenti autologhi: al momento del prelievo, un lettore applicato su un computer palmare o PDA procede all'abbinamento sacca-braccialetto.
- gestione emocomponenti omologhi: il procedimento è analogo, ma l'abbinamento della sacca col braccialetto si esegue mediante una procedura esclusiva che utilizza i transponder applicati alle provette contenenti i campioni di sangue del paziente.
- trasfusione: prima di infondere, un identico lettore legge entrambi i transponder per verificare l'abbinamento e consentire la trasfusione.

Vantaggi:

- tracciabilità completa del processo trasfusionale;
- maggiore efficienza e sicurezza del processo trasfusionale: in caso di anomalie il sistema dà segnalazione visiva e acustica;

- tecnologia non invasiva nei confronti dei degenti;
- maggiore e migliore capacità di intervento nei confronti dei pazienti impossibilitati a interagire con gli operatori sanitari.

10. Altre tecnologie

Nel settore scientifico trattato la letteratura sicuramente è carente, appunto per l'evoluzione e il progresso incombente, gli autori non riescono a stare al passo con il cambiamento e l'innovazione tecnologica che a volte ci sovrasta. In tale contesto è opportuno avere un quadro quanto più completo possibile degli strumenti tecnologici esistenti e sperimentati al fine di eliminare o comunque limitare e prevenire il rischio di eventi avversi o errori. In questo paragrafo sarà analizzato il sistema di sicurezza dell'U.O. trasfusionale in uso presso il Centro Trasfusionale dell'Ospedale Maggiore di Bologna.
Le strategie di prevenzione dell'errore prevedono vari sistemi e strumenti, sia di tipo organizzativo sia di tipo tecnico e tecnologico. L'attenzione di questo documento è centrata prioritariamente sulle soluzioni tecnologiche in grado di limitare l'evento avverso, in particolare su quelle più innovative a radiofrequenza, gli RFId appunto. I software circolanti nei centri trasfusionali possono, con l'ausilio di dispositivi a codici a barre, ridurre l'incidenza degli errori, grazie al controllo automatico delle singole fasi ed, in ultimo, tramite un controllo incrociato al momento della trasfusione. Tali sistemi, comunque, per poter essere sfruttati in ogni loro potenzialità, necessiterebbero di essere integrati con tutto il sistema informativo ospedaliero. Un altro limite riguarda le basse possibilità di controllare e intercettare gli errori commessi al momento del prelievo dei campioni, o al letto del paziente in sede di trasfusione. I sistemi a codice a barra si basano sull'utilizzo di braccialetti identificativi, e di etichette identificative per moduli e provette; risultano essere efficaci se vengono rispettate tutte le procedure operative, ma il loro livello di sicurezza può essere annientato dall'errore dell'operatore in qualsiasi fase del processo trasfusionale.
In alternativa al codice a barre è ora possibile utilizzare dei sistemi di identificazione automatica con tecnologia RFId. Tali dispositivi sono ancora poco utilizzati, e sono attualmente in corso alcune sperimentazioni pilota in alcuni Ospedali Italiani.
Si suppone che in un futuro non molto remoto, grazie anche alle pressioni delle aziende produttrici, tali tecnologie cominceranno presto a diffondersi sia nell'ambito dell'identificazione delle unità di emoderivati, che dei pazienti e del personale sanitario. Attualmente in Italia, nella maggior parte dei centri trasfusionali, per il controllo di tutte le fasi del processo trasfusionale, dalla donazione alla trasfusione, vengono utilizzati dei sistemi a codice a barre abbinati talvolta a dei sistemi meccanici di chiusura che servono ad impedire la trasfusione nel caso in cui il controllo incrociato sangue/paziente rilevi un errato abbinamento.

10.1 Il sistema CARU

I sistemi usati nell'ambito di una sperimentazione su questo tipo di tecnologia sono diversi ma hanno uno stesso fine, andiamo ad analizzare e valutare il sistema CARU.

Questo sistema prodotto dalla TIOMED s.r.l. di Trento è uno dei pochi ad essere munito di una barriera elettromeccanica che impedisca fisicamente la trasfusione di "sangue sbagliato". Esso è formato da:

- Un braccialetto, munito di chip e codice a barre;
- Un palmare munito di stampante di codice a barre;
- Una barriera elettromeccanica, dispositivo che serve a bloccare fisicamente le sacche di sangue ed a registrare nella sua memoria interna gli eventi trasfusionali.

La gestione dei dati viene eseguita tramite il computer palmare denominato Tiddy ed il suo relativo software. L'identificazione del paziente è affidata ad un braccialetto in plastica a chiusura fissa, dotato di un chip elettronico sul quale è prestampato come barcode un codice identificativo univoco (PID). La memoria di cui il chip è dotato, di tipo non riscrivibile, permette, previo collegamento fisico con il palmare, di immagazzinarvi le informazioni aggiuntive relative al paziente (dati anagrafici, codice nosografico, gruppo sanguigno). Il palmare, munito di stampante di codice a barre, è predisposto per produrre direttamente al letto del paziente le etichette necessarie per l'invio al SIT dei campioni necessari per i controlli (provette da 10 ml contenenti un anticoagulante, per l'esecuzione delle eventuali prove crociate e la determinazione del gruppo sanguigno). Prima della consegna al reparto, all'interno del centro trasfusionale, le sacche testate ed assegnate al paziente, vengono inserite all'interno di buste di plastica a chiusura ermetica e, bloccate con un dispositivo elettromeccanico (Bobby), comandato dal PC su cui è residente il software applicativo. La chiusura della sacca di plastica viene effettuata collegando il codice PID del paziente con quello della sacca di sangue; l'operatore, letti i due codici, è in grado di chiudere la barriera fisica, e di caricare i dati sul chip del dispositivo e nel database del sistema. In sede di trasfusione il palmare viene collegato al braccialetto del paziente, ed al Bobby che chiude la busta: se i codici vengono riconosciuti, ed il tempo intercorso dall'imbustamento è inferiore alle 72 ore (tempo di validità della prova crociata), allora viene dato l'impulso che sblocca la barriera e permette che il sangue possa essere trasfuso. Alla fine della procedura il bobby viene riportato al SIT che aggiorna il database inserendovi tutti i dati contenuti nella memoria del dispositivo, compresi gli eventuali tentativi

di apertura della barriera su un paziente sbagliato, e la conferma dell'avvenuta trasfusione, che è obbligatoria per legge. Il sistema provvede anche alla stampa di un'etichetta, da inserire nella cartella clinica del paziente, contenente tutte le informazioni relative al processo conclusosi e le eventuali reazioni post-trasfusione.
Questo tipo di tecnologia viene definita "mista", in quanto presenta sia le caratteristiche di un sistema di identificazione a codici a barre sia con barriera elettromeccanica.
Indubbiamente il sistema CARU risulta essere, tra tutti i sistemi non utilizzanti tecnologie a radiofrequenza, il migliore ausilio disponibile per centri trasfusionali; il suo algoritmo ed i suoi principi di funzionamento sono stati perfezionati grazie alla collaborazione tra la ditta Tiomed ed il personale del SIT dell'Ospedale Maggiore di Bologna, sperimentandolo con due reparti ad alto utilizzo di emocomponenti (Terapia Intensiva e Rianimazione), e ha accumulato l'esperienza di più di 3.000 episodi trasfusionali (di emazie prive di leucociti e plasma) gestiti con questo sistema.
Questo sistema presenta innumerevoli vantaggi, tra cui su tutte, la presenza di una barriera fisica che impedisce errore in sede di trasfusione; la semplicità di funzionamento, l'interfacciabilità con i sistemi gestionali del SIT e la possibilità di estenderne l'utilizzo alla distribuzione dei farmaci ne fanno un ottimo strumento in grado di garantire ottimi livelli di sicurezza trasfusionale senza contare che è utilizzabile anche nei piccoli centri dove non c'è connessione online (i Bobby riportano comunque i dati al SIT). Purtroppo l'evoluzione tecnologica, e la sperimentazione di sistemi RFId, hanno contribuito a rendere tale sistema ormai obsoleto: i controlli da parte del personale sanitario devono ancora essere effettuati manualmente, richiedendo inoltre un elevato livello di attenzione e, per alcune fasi, anche tempi di esecuzione di una certa consistenza, basti pensare alla fase di imbusta mento e chiusura dei Bobby che richiede tempo agli operatori del SIT.

10.2 Le prime sperimentazioni dell'RFId (il sistema BASICHEMO)

Da qualche anno, in Italia, alcuni importanti centri trasfusionali hanno cominciato a sperimentare l'introduzione di sistemi di identificazione automatica nei processi emotrasfusionali, integrando agli ormai collaudati codici a barre, le più recenti tecnologie RFId. Come già descritto in precedenza, presso il SIT dell'Ospedale Maggiore di Bologna, in collaborazione con la ditta Tiomed, è stato avviato il progetto BASICHEMO che risulta attualmente sospeso, anche se le previsioni sono quella di una immediata ripresa per poter continuare la sperimentazione avviata.
È un sistema di sicurezza trasfusionale e fornisce soluzioni ai problemi di identificazione positiva (dei pazienti, dei campioni, dei prodotti biologici, dei farmaci, ecc.) e di comunicazione che spesso sono alla base di errori e di incidenti molto gravi. Il sistema si inserisce nei normali processi di lavoro con una serie di funzioni (codici univoci, "forcing functions", redundancies, barriere fisiche, ecc), atte a prevenire gli errori attivi ed a proteggere il paziente da incidenti provocati da errori eventualmente sfuggiti alla prevenzione. Alla base del funzionamento c'è

innanzitutto un'attenta analisi dei processi trasfusionali a cui si accompagna la disponibilità di strumenti elettronici ed informatici avanzati in grado di fornire risposte tecnologicamente adeguate.

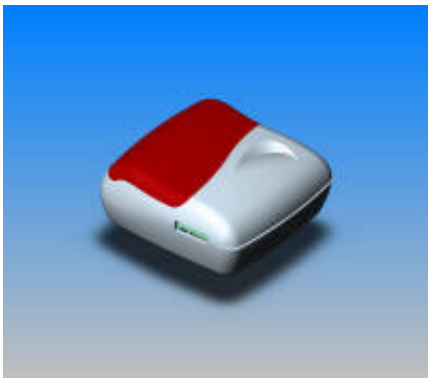
Nato come evoluzione logica del CARU, sfrutta appieno le risorse offerte dal progresso nell'ambito dell'identificazione automatica, utilizzando i più innovativi ed avanzati ritrovati tecnologici, come il bluetooth e il sistema di identificazione mediante riconoscimento delle impronte digitali, applicando il principio di identificazione dell'emoderivato, non più associandolo al codice nosologico identificativo del paziente, ma utilizzando con un codice apposito e non necessitando inoltre della produzione di etichette in sede di prelievo.

Il sistema è composto da:

- un palmare multifunzione, detto PALMED, che gestisce l'intero sistema: legge i braccialetti identificativi muniti di codice a barre o trasponder RFId; comunica con il sistema sia a radiofrequenza, sia ad infrarossi e sia tramite l'interfacciamento ad una porta smart-card; gestisce il database pazienti, e, permette il riconoscimento sia de paziente che dell'operatore, attraverso la lettura dell'impronta digitale e registra addirittura le variazioni di temperatura fisiologica del paziente;
- una postazione informatica situata all'interno del SIT, che è il centro operativo e di gestione di tutto il sistema, munita, del software di gestione del processo e di una interfaccia per la comunicazione senza fili con i palmari (wireless);
- un dispositivo elettronico, detto Medilock, che funge da barriera fisica, permettendo cioè di bloccare la busta in cui viene inserita l'unità ematica, e ne consente lo sblocco solo tramite controllo computerizzato, registra tutti gli eventi trasfusionali, fungendo da ponte tra il palmare ed il centro trasfusionale;
- braccialetti identificativi in plastica a chiusura fissa (removibile cioè solo se tagliato) che integra un trasponder RFId contenente il codice identificativo del paziente (detto PID);
- buste trasparenti, all'interno delle quali vengono allocate le sacche erogate dal centro trasfusionale, che una volta bloccate con il sistema Medilock, possono essere aperte, rendendone utilizzabile il contenuto, solo in sede di trasfusione, e previo un controllo informatizzato delle compatibilità.

Il funzionamento del sistema non è particolarmente complesso, non essendo troppo dissimile, nella sostanza, da quello precedentemente analizzato. Il paziente viene identificato per mezzo del braccialetto contenente l'etichetta RFId; i dati identificativi vengono (in reparto) registrati dal palmare e successivamente comunicati a radiofrequenza alla postazione informatica, che provvede ad associare, ad ogni singolo paziente, il codice PID. La richiesta di trasfusione ed i relativi campioni per le prove di compatibilità vengono fatte automaticamente, associando il PID ai codici a barre presenti già sulle provette e sulla richiesta cartacea. Tutte queste informazioni vengono poi ritrasmesse al SIT che provvederà all'assegnazione del sangue, dopo aver associato anche le sacche selezionate al PID, ed all'effettuazione delle prove di compatibilità o gli ulteriori controlli necessari.

Terminati i controlli di routine, le sacche vengono inserite nell'apposta busta trasparente, e quindi bloccate informaticamente e fisicamente con il Medilock, all'interno del quale tramite il PC, si provvederà via wireless, ad inserire la combinazione di sblocco.



L'apertura della busta avviene infine, in sede di trasfusione, mediante il palmare viene riconosciuta la congruità tra il codice contenuto nel braccialetto del paziente afferente e quello contenuto sul dispositivo di chiusura, rende disponibili le unità di sangue o plasma da trasfondere sbloccando il Medilock. Durante la procedura di sblocco, il palmare effettua inoltre un ulteriore controllo incrociato del gruppo sanguigno (tramite l'adozione di barcode di gruppo a codice UNI), assicurando l'apertura della busta solo in caso di assoluta compatibilità. Tutti gli eventi memorizzati nel Medilock, una volta che quest'ultimo viene restituito al SIT, vengono inseriti nel database grazie ad una semplice lettura ottica comunicando con il PC tramite bluetooth.
Attualmente non esistono esperienze pratiche di utilizzo di tale sistema o per lo meno non esistono dati statisticamente rilevanti in quanto la sperimentazione risulta sospesa in attesa che l'azienda produttrice garantisca la necessaria collaborazione al centro trasfusionale. Durante l'intero periodo di sperimentazione sono emerse tutte le qualità del sistema, comprese rapidità, precisione, semplicità d'uso, oltre che le potenzialità di sistema universali di identificazione del paziente, e le maggiori garanzie per la sicurezza trasfusionali.
Tale sistema, come già detto, rappresenta la sintesi di tutti i più avanzati principi di gestione del rischio trasfusionale, racchiudendo in sé una barriera fisica efficace, una totale tracciabilità,

controlli incrociati informatizzati e identificazione dei campioni per mezzo di codici provetta, oltre che i più recenti ritrovati tecnologici, quali i dispositivi RFID, le comunicazioni senza fili e ad infrarossi, nonché la lettura di impronte digitali. A tali vantaggi si associa inoltre una completa integrabilità con i gestionali dei SIT, una semplicità d'uso che non richiede una particolare formazione del personale sanitario, ed una dotazione hardware essenziale e non troppo dispendiosa. Ad oggi purtroppo mancano ancora dati relativi all'esperienza d'uso che possano permettere un'analisi più accurata di tale tecnologia, anche se da un primo studio sembra che l'unica criticità che esso presenta, sia la richiesta di tempo-lavoro per l'operazione di imbusta mento delle sacche, effettuata manualmente dall'operatore, e la successiva chiusura tramite il Medilock, effettuata sì elettronicamente, ma previo inserimento del dispositivo nell'apposita postazione collegata al PC.

11. Il sistema Gricode

Il Gricode è un sistema studiato per ottenere la massima sicurezza della procedura trasfusionale con la massima semplicità ma applicabile ad altre realtà in ambito sanitario.
Si compone di quattro parti:
1. Braccialetto in Tyvek con chiusura di sicurezza;
2. Etichette Barcode prestampate;
3. Lettore portatile di etichette Barcode;
4. Software di Gestione del Sistema.

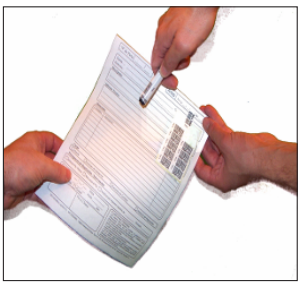
Gricode Prelievo - Richiesta:

- Verifica congruità tra codice di sicurezza:
  1. Paziente (braccialetto)
  2. Provetta campione
  3. Richiesta Emocomponente

- Il Sistema registra
  1. Reparto
  2. Operatore
  3. Ora e Data Prelievo
  4. Numero Richiesta/Provetta
  5. Numero Paziente (facoltativo)

Gricode Accettazione – Registrazione:

- Verifica congruità tra codice sicurezza:
  1. Provetta
  2. Richiesta Emocomponente



- Il Sistema registra:
  1. Operatore

2. Ora e data della Ricezione
3. Numero della richiesta

Gricode Distribuzione Emocomponente:

- Verifica congruità tra codici:
  1. Codice di sicurezza
     (sacca / richiesta trasfusionale)
  2. C.D.M.

(etichetta donazione/assegnazione)

- Il Sistema registra:
  1. Operatore
  2. Ora e Data di Distribuzione
  3. Numero della sacca distribuita
  4. Tipo Emocomponente

Gricode Inizio Trasfusione:

- Verifica congruità tra codici:
  1. Codice di sicurezza
     (sacca / braccialetto paziente)
  2. C.D.M.

  (etichetta donazione/assegnazione)

- Il Sistema registra
  1. Reparto
  2. Medico
  3. Operatore (Facoltativo)
  4. Ora e Data inizio Trasfusione
  5. Numero sacca da Trasfondere
  6. Tipo emocomponente trasfuso

Gricode Emovigilanza:

- Termine Trasfusione
- Il Sistema registra:

1. Reparto
2. Operatore
3. Ora e Data
4. Numero sacca Trasfusa
5. Tipo di emocomponente Trasfuso
6. Esito della Trasfusione
7. Eventuali Reazioni Avverse

12. Implementazione e costi di un sistema Gricode

In questo paragrafo, per esplicitare il basso costo e la semplicità applicativa di un sistema RFId, Gricode o in linea generale un sistema che utilizza tecnologie avanzate, sarà riportato l'esempio di sperimentazione utilizzato presso la AUSL 21 di Legnago.
L'azienda in questione ha installato il sistema Gricode nel 2008, che dopo un periodo di prova di tre mesi, è diventato operativo routinariamente. Nell'anno 2009 si sono Bovolone che sperimentalmente hanno introdotto il sistema in due unità operative. Per opportunità, i professionisti hanno ritenuto di dovere interfacciare il sistema Gricode con un altro sistema di gestione e organizzazione della struttura sanitaria denominato Cetraplus. Chiaramente le prime difficoltà sono state superate con successo, in quanto, come spesso accade quando si apportano delle innovazioni in un sistema, si è trovata una resistenza di alcuni operatori sanitari, sono stati commessi errori procedurali e di lettura dei codici, nonché, vi sono state difficoltà nell'elaborazione dei dati statistici. Superata questa fase sono stati ottenuti i primi risultati, ossia, sono stati evitati numerosi Near misses.
In particolare, nell'anno 2009 il sistema Gricode ha evitato agli operatori errori di etichettatura in distribuzione, errori di identificazione del paziente, errori connessi a scambi di provetta al momento dell'accettazione del campione.
Quindi il primo aspetto che emerge è connesso alla tutela della salute dei pazienti-utenti, di conseguenza, la tutela degli operatori sanitari da eventuali contenziosi, tutela dell'azienda sanitaria che subisce il costo economico del contenzioso ma anche, da un punto di vista morale la perdita di fiducia verso l'azienda riduce quel valore immateriale, che ad esempio, le grandi industrie acquisiscono dopo decenni di investimenti (c.d. brand).
Per ultimo, apparentemente scioccante è il costo dell'implementazione di un sistema di sicurezza ad alto contenuto tecnologico che ammonta per il 2009 a 20.000 mila euro per singola unità operativa.
Approssimativamente il costo e l'installazione di un sistema RFId si allinea a quello Gricode, descritto pocanzi, con la differenza che l'RFId è sostanzialmente estendibile a tutte le realtà in ambito sanitario (si pensi al conteggio di garze, strumenti, ed altro in fase operatoria).
Dobbiamo porci soltanto una domanda alla quale ognuno di noi può rispondere senza la necessità di particolari studi scientifici, perché i costi sanitari sono elevatissimi e quando si verificano delle implementazioni di sistemi altamente tecnologici che costano molto poco non si adottano tali strumenti in modo sistematico ? Perché si avverte la necessità del cambiamento e del miglioramento soltanto in poche e piccole realtà territoriali e tali approcci vengono spesso recepiti come attività sperimentali e non prassi definitive ?

2.3 SICUREZZA E PRIVACY

Il ciclo di vita di una etichetta è sicuramente superiore a quello degli oggetti a cui essa viene associata, avendo una aspettativa di vita teoricamente infinita. Sarebbe quindi possibile, anche dopo che gli oggetti escono dalla catena di distribuzione, continuare ad interrogare i trasponder, e raccogliere informazioni sulle abitudini degli stessi proprietari.
Per tale motivo è molto acceso il dibattito sulla privacy nei sistemi di identificazione a

radiofrequenza, che tende a focalizzarsi sulle applicazioni dei trasponder a singoli articoli di consumo e agli oggetti comunemente in possesso di privati. E' così che l'etichettatura elettronica, seppur non ancora massicciamente diffusa, genera timori connessi al potenziale uso che le aziende potrebbero fare di queste apparecchiature, utilizzandole per acquisire informazioni indebite alla clientela. In Italia queste problematiche sono state affrontate dal Garante per la Protezione dei Dati Personali in un provvedimento a carattere generale – Garanzie per l'uso di "etichette intelligenti" – del 9 marzo 2005. Questo provvedimento definisce le misure per rendere il trattamento dei dati personali nelle tecnologie RFID conforme alle vigenti disposizioni.
Una tecnologia che non prevede né il contatto fisico né la visibilità tra gli apparati favorisce indubbiamente la possibilità di poter acquisire dati in maniera fraudolenta, o eventualmente alterarli o distruggerli.
Sfortunatamente non sono ancora molte le misure di sicurezza attuabili per proteggere il sistema da eventuali manomissioni. Esistono comunque soluzioni che si sono rilevate più efficaci della semplice password, come ad esempio i metodi di crittografia utilizzati nelle transazioni finanziarie.

2.4 COSTI E SVILUPPO

I costi di un sistema RFID possono essere così ripartiti:

- Costo del software: 7%
- Costo dei servizi: 34%
- Costo dell'hardware: 59%

La diffusione dei sistemi RFID (soprattutto nella grande distribuzione) è stata a lungo ostacolata dai costi dei singoli componenti. Da tempo si considera come soglia accettabile per le "etichette intelligenti", il costo di 5 centesimi di euro per unità, ma attualmente il costo si aggira tra i 20 centesimi fino a 50 euro (se con batteria integrata), da 500 a 3000 euro per i lettori (in base alla funzionalità). A questo si contrappone il costo irrisorio delle etichette con codice a barre (meno di 1 centesimo ciascuna).

2.5 APPLICAZIONI

La continua evoluzione della tecnologia e della scienza che ne è supporto, in particolare quella della miniaturizzazione e dei superconduttori, fornisce sempre nuovi strumenti hardware idonei a consentire un miglior sviluppo delle tecnologie di gestione dei progetti di impresa, in cui indubbiamente, ha avuto un ruolo fondamentale, la rivoluzione epocale avutasi a seguito della riduzione dei prezzi di commercializzazione dei dispositivi RFID. In un mondo in cui un dirigente debba prendere decisioni il più possibile basate su fatti piuttosto che su previsioni, questo debba conoscere e rispondere alle condizioni di mercato, fare piani ed eseguirli, e soprattutto imparare dalla propria esperienza; un sistema composto da parti automatizzate ed intelligenti può condurre eccezionali e nuovi livelli di efficienza, coordinazione e collaborazione nel sistema di una rete commerciale adattiva.
I campi di applicazione dell'RFID sono potenzialmente illimitati. Uno dei principali settori in cui vengono utilizzati questi dispositivi è ovviamente la Sanità. Alcuni esempi di applicazione sono: il monitoraggio oculistico, le sonde sottocutanee, l'identificazione e la tracciabilità di

pazienti, farmaci, attrezzature e operatori, la gestione dei farmaci, processi trasfusionali e prevenzione di errori clinici.

13. La terza industria del settore sanitario europeo

Secondo uno studio recente[20] la sanità elettronica sta diventando una vera e propria nuova industria accanto a quella farmaceutica e dei dispositivi medici. Entro il 2010 essa potrebbe assorbire il 5% del bilancio complessivo della sanità dei 25 Stati membri, contro appena l'1% del 2000 (nell'Unione a 15)[21]. Le aziende europee hanno tutte le possibilità di diventare leader mondiali in questo nuovo settore. Le tecnologie dell'informazione e della comunicazione hanno svolto un ruolo determinante nel settore farmaceutico e dei dispositivi medici. I ricercatori farmaceutici utilizzano le nuove tecnologie per simulare e aggregare dati clinici sperimentali e per verificare nuove teorie. I più recenti dispositivi medici sono dotati di software sofisticati che li rendono più sicuri ed efficaci (grazie ad esempio al monitoraggio a distanza delle funzioni) e costituiscono un supporto decisionale per i medici e/o i pazienti.

Conclusioni

L'introduzione di nuove tecnologie di identificazione automatica a radiofrequenza ha permesso un considerevole passo avanti in materia di sicurezza nel settore sanitario, tali sistemi si sono dimostrati efficaci ed efficienti nella prevenzione degli eventi avversi, degli errori, e quindi sono stati tutelati i pazienti/utenti ma anche le aziende sanitarie dall'innumerevole quantità di procedimenti penali e civili derivanti da danni arrecati a persone che negli ultimi anni sono diventati un costo insostenibile per le amministrazioni pubbliche, ma anche per le assicurazioni, non più disposte a emettere polizze a coperturadi questa tipologia di eventi. Attualmente non sono molti i centri in Italia che utilizzano sistemi di sicurezza basati su tecnologie RFId, ma paradossalmente potrebbe costituire un vantaggio per poter intervenire immediatamente ed omogeneamente su tutto il sistema sanitario nazionale pubblico e privato con tecnologie e sistemi univoci, implementabili con tecnologie alla portata di tutte le aziende (un computer, un palmare, un telefono, con connessione bluetooth o wifi) che comunicando con applicativi che utilizzano i sistemi RFId permetterebbero di salvare una infinità di vite umane, di ridurre i costi sanitari motivo di acceso dibattito, anche politico, negli ultimi anni, ma principalmente si potrebbe creare quel clima di fiducia nei confronti di un ottimo sistema sanitario da riorganizzare ponderando l'uso delle risorse. Una riflessione è d'obbligo, se pensiamo che

---

[20] Deloitte e Touche (2003) *e*Health. *Health Information Network Europe. Final report;*

[21] *The European e-Business Report - 2002/2003 edition. A portrait of e-business in 15 sectors of the EU economy* – Prima relazione di sintesi dell'e-Business W@tch. Lussemburgo: Ufficio delle pubblicazioni ufficiali delle Comunità europee, 2003. ISBN 92-894-5118-1; Empirica, SIBIS, *Benchmarking Highlights 2002: Towards the Information Society in Europe and the US*, maggio 2003. Si veda: http://www.sibis.org/.;

l'Italia è l'unico paese dove le prestazioni sanitarie hanno un costo irrisorio, in alcuni casi inesistente a fronte di altri paesi come gli Stati Uniti dove le prestazioni sono totalmente a carico del paziente/utente, o di altre realtà Europee dove molti interventi chirurgici ed altre prestazioni hanno un costo elevato e diretto per il paziente/utente. In tal senso il Consiglio Europeo, il Parlamento Europeo e le Commissioni sono più volte intervenute con atti ufficiali, appunto per porre in essere tutte quelle attività scientifiche, tecnologiche ed operative, tendenti a tutelare la salute dei cittadini. Questo intervento è parte integrante delle politiche europee e spesso ha raggiunto il territorio con apposite comunicazioni ufficiali rivolte alle Regioni. Oggi le Regioni sono il punto focale della gestione e delle politiche sanitarie, su di esse grava la responsabilità dei programmi, della sicurezza e della spesa connessa alle aziende sanitarie. Il messaggio Europeo è chiaro, adeguandosi ai protocolli di sicurezza degli utenti che tutelano la salute del paziente/utente, di riflesso sono stati tutelati i professionisti che operano in tale contesto, le aziende e nel lungo periodo tali politiche potranno beneficiare di una sensibile riduzione della spesa sanitaria.

E' evidente che per molti anni il maggiore impedimento per la diffusione di nuove tecnologie all'interno delle aziende sanitarie è stato costituito dal costo dei dispositivi, non sempre corrispondente alla disponibilità di investimento delle strutture stesse, a volte l'elevato costo è stato utilizzato come strumento di governante del "non facere". Attualmente l'indirizzo delle industrie del settore è cambiato, oggi l'abbattimento dei costi, possibile anche con adeguate economie di scala, ha permesso la nascita di sistemi sperimentali che grazie anche a normative di tipo regionale o meglio ancora nazionale, possano diffondersi rapidamente, garantendo all'utente sanitario del ventunesimo secolo la sicurezza, la tutela della salute e l'affidabilità proprie di società evolute con tecnologie all'avanguardia. Sembra quindi inevitabile ed è auspicabile che presto il dispositivi RFId verranno integrati agli attuali sistemi a disposizione in tutte strutture sanitarie, essendo infatti possibile integrare tali tecnologie, che ben si prestano a numerose altre applicazioni, con i sistemi informatizzati delle Unità sanitarie stesse.

BIBLIOGRAFIA

A. Alfano (2006); Sicurezza ed interoperabilità dei sistemi RFId, Dip. Inform. Università La Sapienza-CNIPA;

L. Battezzati, J. L. Hygounet (2006); RFID. Identificazione automatica a radiofrequenza Seconda Edizione Ulrico Hoepli Editore s.p.a.;

D.W. Bates, A.A.Gawande (2003); Patient safety: Improving safety with information technology. *New England Journal of Medicine*;

CNIPA (2006); Le tecnologie RFID e le offerte del mercato;

Commissione Europea, COM(2000) 285; programma d'azione comunitario nel campo della sanità pubblica (2001-2006);

Commissione Europea, COM(2000) 285; Sanità elettronica – migliorare l'assistenza sanitaria dei cittadini europei;

Commissione Europea, COM(2007) 630; Libro Bianco Un impegno comune per la salute: Approccio strategico dell'UE per il periodo 2008-2013;

Commissione Europea, COM(2008) 725; Libro Verde relativo al personale sanitario europeo;

http://www.pubblicaamministrazione.net/infrastrutture-it/articoli/632/le-applicazioni-rfid-nella-sanita-pubblica.html "Le applicazioni RFID nella sanità pubblica";

International Conference on Personal Wireless Comunications - PWC'06, September (2006); Survey on Security Threats and Proposed Solutions;

P. Peris-Lopez, J. C. Hernandez-Castro, J. Estevez Tapiador, A. Ribagorda. (2006); RFID Systems: A

A. Serbanati (2006); RFID Security;

ALLEGATO TECNICO[22]

L'*Identificazione* a *Radio Frequenza* è una tecnologia per la identificazione automatica e remota di oggetti, soggetti, animali che usa tag(transponder) interrogati, attraverso un canale a radiofrequenza, da lettori o interrogatori (transceiver):
Un sistema RFID è tipicamente costituito da tre componenti principali: il tag (o trasponder), il lettore (o *transceiver*) e l'infrastruttura software.
Il trasponder viene applicato all'oggetto da identificare, memorizza tipicamente un identificativo univoco (e opzionalmente ulteriori dati) e rappresenta, quindi, il supporto dati reale del sistema. Un trasponder può essere considerato, di fatto, come un supporto passivo che viene letto a distanza e non presenta nessuna capacità di elaborazione propria.
Il lettore è il dispositivo che estrae informazioni dal tag, grazie alla propria antenna che permette che si instauri una comunicazione tra il trasponder e il lettore stesso, tramite radiofrequenza,

[22] Alfano A., Sicurezza ed interoperabilità dei sistemi RFId, Dip. Inform. Università La Sapienza-CNIPA, 2006;

e consente di effettuare operazioni di lettura e, eventualmente, di scrittura.
L'infrastruttura software (ad esempio, un singolo PC o un sistema host) filtra i dati letti, rendendoli disponibili per il sistema informativo aziendale.
In sintesi, quando viene richiesto dall'applicazione, i dati relativi all'asset riportati sul tag vengono "recuperati" mediante l'antenna e il lettore, e raccolti da un sistema di gestione delle informazioni. I dati trattati possono essere di vario tipo: semplici come un numero identificativo o complessi come istruzioni, informazioni sulla spedizione, rapporti sui danni, storia della temperatura.
L'utilità fondamentale di un sistema RFID risiede nella capacità di effettuare una raccolta di informazioni in modo facile. Le informazioni contenute negli oggetti con tag possono essere trasmesse per un insieme di elementi simultaneamente, attraverso barriere e a distanza.
Queste caratteristiche hanno spinto lo sviluppo di tecnologie per un vasto raggio di applicazioni, come vedremo, in diversi campi, ma la stessa semplicità di utilizzo può in qualche modo nascondere le vulnerabilità del sistema.
Pertanto le caratteristiche fondamentali di un sistema RFID sono: la presenza di un identificativo univoco del tag, la presenza di un sistema anticollisione sul tag nella comunicazione tra tag e reader(in quanto ogni lettore può leggere più tag che accedono allo stesso momento, mentre l'anti-collisione permette al tag di comunicare a turno con il lettore), un lettore che sincronizzi la coordinazione ed un middleware che raccolga ed organizzi i dati da inviare al sistema informativo.

Tag: caratteristiche

Un tag consiste di un piccolo micro con la possibilità di memorizzazione dati, limitate capacità di logica ed elaborazione ed una antenna. Ogni oggetto che deve essere identificato in un sistema RFID, deve essere dotato di un tag. I tag vengono realizzati con forme diverse a seconda del tipo di oggetto su cui dovranno essere applicati e sulla base delle condizioni ambientali in cui dovranno essere utilizzati. Esiste, infatti, una vasta gamma di tag che si differenziano tra loro per dimensioni (piccoli come un chicco di riso o grandi come mattoni, abbastanza sottili da identificare un bullone, abbastanza larghi per contrassegnare un vagone ferroviario), capacità di memoria, resistenza alle temperature e molte altre caratteristiche. Al contrario, quasi tutti i tag sono accomunati dal fatto di essere incapsulati al fine di garantirne l'efficienza, assicurandone la resistenza agli urti, allo sporco, agli agenti chimici e all'umidità.
Tra i vari tipi di tag che si differenziano dal punto di vista morfologico ci sono quelli flessibili con forma di carta di credito, quelli con forma di disco e moneta, i tag dedicati (modellati in supporti di plastica usati da contenitori), i tag a forma di chiave, i tag progettati su misura per contenitori e pallet, i tag di carta, ecc.. I tag risultano immuni alla maggior parte dei fattori ambientali, ma i range di lettura e scrittura possono risentire in modo determinante della vicinanza di metalli, di liquidi e di radiazioni elettromagnetiche che ne influenzano le prestazioni, interferendo o assorbendo le onde emesse dal sistema. Per queste ragioni è importante progettare e realizzare singolarmente ogni installazione, poiché sistemi ben progettati e installati sono in grado di sopperire a tali problemi che possono renderli vulnerabili alle minacce di attacchi.
Ogni trasponder è dotato di un proprio codice identificativo univoco fornito dall'azienda che lo produce. Tale codice non è suscettibile di modifiche e non può essere cancellato o

copiato. Ciò fa sì che ciascun trasponder sia unico e, di conseguenza, rende impossibile ogni tipo di contraffazione. C'è un ulteriore codice identificativo progressivo che viene attribuito al trasponder al momento della prima inizializzazione e assegnazione da parte dell'azienda proprietaria del bene.
Quando viene adottata un'architettura distribuita(come descritta in seguito), viene creato un vero e proprio database remoto che si muove insieme al bene, grazie al fatto che il trasponder è solitamente fissato sul prodotto o, per lo meno, sul dispositivo di trasporto.
Le cosiddette *labels* (etichette) e le PCB (*Printed Circuit Boards*, schede a circuito stampato) rappresentano due formati particolari di tag. Le prime hanno una bobina a radiofrequenza stampata, punzonata, impressa o depositata su un substrato di carta o di poliestere con un chip di memoria. Una label è meno resistente alle condizioni ambientali rispetto a un tag incapsulato, ma vantaggiosa economicamente in ambiti applicativi in cui non sia previsto il riutilizzo del trasponder e si abbia a che fare con alti volumi.
Le PCB sono destinate ad essere incorporate nei prodotti o nel vettore e, pur presentando ottime caratteristiche di resistenza alle alte temperature, richiedono di essere incapsulate nell'eventualità che entrino in contatto diretto con le condizioni ambientali esterne come, ad esempio, pioggia o eccessiva umidità. Una PCB, quindi, presenta soprattutto una grande vantaggio, che consiste nella resistenza in ambienti in cui una semplice label non sarebbe in grado di sopravvivere.
Un tag si compone, a sua volta, di un chip, di un'antenna e di un supporto fisico. Il chip consente di gestire le attività di comunicazione e identificazione e ha il compito di aumentare la capacità di memorizzazione del trasponder. L'antenna è l'apparato che consente al tag di essere alimentato (qualora non sia equipaggiato con una batteria) e di ricevere e, eventualmente, trasmettere informazioni da e per il mondo esterno. Il supporto fisico consiste nel materiale che sostiene e protegge il sistema composto dal tag e dall'antenna. Per quanto riguarda la potenza di calcolo, si cerca di ottenere consumi di potenza molto bassi, soprattutto nel gestire i segnali a radiofrequenza rumorosi e nel rispettare le stringenti disposizioni in termini di emissioni. I tag sono realizzati in tecnologia CMOS e la maggior parte di essi contiene una certa quantità di memoria non volatile (NVM, *Non Volatile Memory*), come le EEPROM, al fine di immagazzinare i dati in quantità che va da 96 bit a 32 Kbit. a maggiori dimensioni della memoria corrispondono dimensioni maggiori del chip e, quindi, un maggior costo del tag.
Ponendo l'attenzione alle modalità di alimentazione elettrica e di trasmissione rispetto al lettore, è possibile distinguere i tag in passivi, semiattivi e attivi.
Il *tag passivo,* utilizzato tipicamente per le applicazioni di massa come mezzi di trasporto a bassa velocità, identificazione di persone o cose, ecc. dipende per l'alimentazione dal lettore, riceve cioè energia dalla stessa antenna di lettura, il lettore RFID trasmette un fascio di energia che "sveglia" il tag e fornisce al chip la potenza, estratta dalle onde elettromagnetiche, necessaria per trasmettere i dati. La capacità di trasmissione risulta quindi limitata ai momenti in cui il tag viene interrogato. Il vantaggio di diminuire il costo unitario del tag va cioè a discapito delle prestazioni.
La comunicazione avviene a distanze che vanno da qualche centimetro a qualche metro a seconda della frequenza di lavoro.
I *tag semiattivi (o semipassivi)* vengono usati per applicazioni speciali (è il caso del telepass e dei

vagoni ferroviari). Questi trasponder hanno batterie incorporate (anche se con un'autonomia limitata) per l'alimentazione dei circuiti, ma sono in grado di trasmettere dati solo se interrogati dal lettore perchè non sono dotati di un trasmettitore integrato e per questo sono ancora costretti ad usare il campo generato dal lettore per effettuare la trasmissione. Lo scopo che si vuole raggiungere mediante l'utilizzo di questa tipologia di tag è ottenere un miglioramento nelle prestazioni rispetto ai tag passivi, in particolar modo per quanto riguarda la portata operativa, infatti la comunicazione può avvenire a distanze di alcune decine di metri (tipicamente 15 metri), in conseguenza del fatto che questi tag possono funzionare con livelli più bassi di potenza del segnale.
Per i *tag attivi* si ha a che fare con applicazioni sofisticate, quali aerei militari e civili e mezzi di trasporto in movimento a velocità elevate, per applicazioni che cioè richiedono funzionalità evolute come, ad esempio, nel caso in cui sia richiesto un controllo continuo di grandezze fisiche (ad esempio la temperatura di un contenitore refrigerato, pressioni, ecc..). Sono dotati di una fonte di alimentazione indipendente dal lettore, in quanto posseggono una batteria che sfruttano sia per alimentare i circuiti interni del chip che per le operazioni di trasmissione dei dati al lettore. Trasmettendo autonomamente i dati, le prestazioni sono caratterizzate da comunicazioni effettuate a distanze che vanno dalle decine di metri alle decine di chilometri.

Le differenze tra tag passivi, semiattivi e attivi sono riassunte nella Tabella che segue:

TAG	VANTAGGI	SVANTAGGI	OSSERVAZIONI
Passivi	- tempi di vita più lunghi - vasta gamma di forme - meccanicamente più flessibili - basso costo	- distanze limitate a 4-5 metri - controllati dalle regolamentazioni locali	- sono i più usati nei sistemi RFID - bande LF, HF, UHF
Semiattivi	- grande distanza di comunicazione - possibilità di uso per controllare altri dispositivi come i sensori (temperatura, pressione, ecc..)	- costosi a causa della batteria e del contenitore - affidabilità: impossibile determinare se una batteria sia buona o difettosa, specialmente negli ambienti con tag multipli	- usati principalmente nei sistemi in tempo reale per rintracciare materiali di alto valore. I tag sono UHF
Attivi	- non rientra nelle stesse regolazioni rigorose di alimentazione imposte ai dispositivi passivi	- la proliferazione di trasponder attivi presenta un rischio ambientale, di prodotti chimici potenzialmente tossici usati nelle batterie	- usati nella logistica per rintracciare container sui treni, camion, ecc..

Rivista elettronica di Diritto, Economia, Management

N. 1 - 2010 · pp. 243-277

La sicurezza informatica
Profili giuridici, Standard e Modelli di gestione

Claudia Ciampi

Abstract: Nell'ultimo ventennio il mondo delle comunicazioni, delle transazioni e più in generale dei rapporti interpersonali, ha subito enormi cambiamenti. Si è assistito ad una crescente diffusione delle tecnologie informatiche e telematiche, all'utilizzo della rete sia per lo scambio di beni, materiali o immateriali, che per l'erogazione di servizi, ad una transizione sempre più netta che ha visto i processi aziendali passare da una modalità cartacea e vocale ad una modalità completamente informatica. Tale evoluzione, se da un lato ha comportato notevole vantaggi per le organizzazioni sia pubbliche che private, dall'altro le ha esposte a numerosi rischi di natura informatica potenzialmente dannosi per la riservatezza, l'integrità e la disponibilità del patrimonio informativo. La crescita dei pericoli in grado di compromettere la sicurezza dei sistemi informatici, rappresenta un'inquietante minaccia ed un forte ostacolo alla creazione ed allo sviluppo della società dell'informazione. Il problema della sicurezza informatica, avvertito tanto nel settore privato quanto nel pubblico, è oggigiorno tra le tematiche più complesse e di difficile gestione.

In the last two decades the world of communications, transactions and more generally of the interpersonal relationship, has undergone enormous changes. There has been an increasing spread of information and communication technologies, using the network for the exchange of goods, tangible or intangible, and for the provision of services, a transition that has been more and more clear changing business processes from paper and voice mode to a completely computer one. This development, while it has brought significant benefits to public and private organizations, expose them to numerous hazards and potentially damaging to the confidentiality, integrity and availability of information assets. The growth of potential danger that compromise the security of computer systems, represents a worrying threat and the major obstacle for the creation and development of the information society. The problem of computer security is warned both in the private and public sector, and today is one of the more complex and difficult issues to manage.

Parole chiave: Sicurezza informatica, Sicurezza delle informazioni, ISO/IEC 27001, Information Security Management System, Politiche di sicurezza, Analisi dei rischi, TCSEC, ITSEC, ISO/IEC 15408, ISO/IEC 27005, ISO/IEC TR 13335.

Articolo pervenuto il 5 ottobre 2010, approvato il 24 novembre 2010

Sommario: 1.Introduzione alla tematica 2.Concetto e rilevanza della sicurezza informatica – 3.Quadro normativo nazionale di riferimento - 4.La posizione dell'Unione Europea. 5.Il contesto internazionale: Gli Standard di sicurezza - 6.Modelli di gestione della sicurezza - 7.Logiche organizzative per i presidi della sicurezza. 8.La Certificazione ISO/IEC 27001 - 9. Conclusioni

1. Introduzione alla tematica

Le crescenti minacce provenienti non solo da Internet (ad es. attacchi, intrusioni e accessi non autorizzati etc..) ma anche dall'interno delle reti (ad es. scorretto utilizzo dei sistemi informatici, diffusione non controllata di dati aziendali, diffusione involontaria di virus etc..) rendono i sistemi informatici più vulnerabili, esponendo le organizzazioni pubbliche e private a nuovi rischi di frodi, furto o diffusione di informazioni, arresto di servizi con prevedibili conseguenze di natura legale o economica, di perdita di immagine o di efficienza.
All'interno di questo complesso scenario, gli aspetti di sicurezza assumono un'importanza fondamentale e la risoluzione delle problematiche legate alla "gestione" ed alla "salvaguardia delle informazioni", anche grazie alla attuale legislazione nazionale, diventa un obiettivo cogente e non più un'opzione di scelta da valutare esclusivamente in termini di costi.
Nessun sistema informatico è probabilmente mai completamente sicuro; anche i sistemi più curati dal punto di vista della sicurezza possono poi rivelarsi vulnerabili, magari da parte di utenti che ancorché autorizzati abusano dei privilegi loro concessi. Quindi, quello che le organizzazioni possono ottenere attraverso una corretta gestione della problematica è di rendere particolarmente difficili i tentativi di compromissione dei sistemi.
Ne consegue che un sistema di gestione della sicurezza può considerarsi "sicuro" soltanto rispetto alla sua capacità di ridurre a livelli accettabili i rischi di compromissione della riservatezza dell'integrità e della disponibilità delle risorse protette.
In questa ottica la sicurezza deve essere considerata "un processo, non un prodotto" [1] e va analizzata ed affrontata attraverso un approccio integrato (tecnologico ed organizzativo, organico, strutturato ed interdisciplinare) ovvero mediante la strutturazione di un processo continuo di identificazione, analisi e valutazione dei rischi, nonché di selezione delle migliore strategie di prevenzione e gestione degli stessi.
L'adozione di tale processo, più comunemente noto come Information Security Management System (ISMS) [2], finisce per costituire un indicatore di efficienza e di solidità dell'organizzazione che sarà in grado di garantire l'affidabilità e la continuità dei servizi erogati, il mantenimento di appropriati livelli di confidenzialità, integrità e disponibilità delle informazioni e conquistare, dunque, la fiducia dei propri clienti/utenti.

---

1 Schneier B., Sicurezza Digitale, Tecniche Nuove, Milano, 2001

2 Standard ISO/IEC 27001:2005 e ISO/IEC 27002:2007

2. Concetto e rilevanza della sicurezza informatica

Con il termine sicurezza informatica, in via generale, si indica quella branca dell'informatica che si occupa della salvaguardia dei sistemi informatici e delle reti da potenziali rischi di acceso, utilizzo, modifica e distruzione sia accidentali che dolosi.
Nel'odierno contesto ICT (Information & Communication Technology), il significato del termine si è andato evolvendo fino a coincidere con quello di "sicurezza dell'informazione" [3].
In tal senso, oggiggiorno per sicurezza informatica si intende la capacità di salvaguardare la riservatezza, l'integrità e la disponibilità delle informazioni, qualunque forma esse assumano e qualunque siano i mezzi con cui vengono condivise o memorizzate, e delle risorse utilizzate per il suo trattamento, contrastando efficacemente ogni minaccia sia di tipo accidentale sia di tipo intenzionale, ovvero riducendo al minimo i rischi attraverso l'individuazione, la realizzazione e la gestione di opportune contromisure di natura fisica logica ed organizzativa[4].
In tale moderna accezione, che trova riscontro sia nel settore privato che in quello pubblico[5], gli obiettivi della sicurezza informatica vengono dunque generalmente espressi in termini di requisiti volti a:

- salvaguardare la *riservatezza* dell'informazione, quindi la sua confidenzialità, riducendo a livelli accettabili il rischio di accesso, volontario o involontario, non autorizzato o di intercettazioni da parte di terzi;
- proteggere l'*integrità* dell'informazione, ovvero la sua "accuratezza", "completezza" e "validità", riducendo a livelli accettabili il rischio di cancellazioni o modifiche non autorizzate da parte di terzi, o del verificarsi di fenomeni non controllabili (come ad esempio il deteriorarsi dei supporti di memorizzazione, la degradazione dei dati trasmessi su canali rumorosi, i guasti degli apparati, i problemi ai sistemi di distribuzione dell'energia, gli incendi, gli allagamenti, etc.) e prevedendo adeguate procedure di recupero delle informazioni (ad es. piani di Disaster Recovery, etc…);
- garantire la *disponibilità* dell'informazione, riducendo a livelli accettabili il rischio che

---

[3] "Information is an asset that, like other important business assets, is essential to an organization's business and consequently needs to be suitably protected. Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or by using electronic means, shown on films, or spoken in conversation. Whatever form the information takes, or means by which it is shared or stored, it should always be appropriately protected" (ISO/IEC 27002:2005).

[4] "Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities.Information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific security and business objectives of the organization are met. This should be done in conjunction with other business management processes" (ISO/IEC 27002:2005).

[5] "Le informazioni gestite dai sistemi informativi pubblici costituiscono una risorsa di valore strategico per il governo del Paese. Questo patrimonio deve essere efficacemente protetto e tutelato al fine di prevenire possibili alterazioni sul significato intrinseco delle informazioni stesse. È noto infatti che esistono minacce di intrusione e possibilità di divulgazione non autorizzata di informazioni, nonché di interruzione e di distruzione del servizio" (Direttiva 16 gennaio 2002 del Presidente del Consiglio dei Ministri "Sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni statali." G.U. 22 marzo 2002, n. 69)

possa essere impedito a soggetti autorizzati l'accesso de il successivo utilizzo delle informazioni e dei servizi ogni qual volta richiesti.

Ove si considerino le informazioni in fase di trasmissione ai sopra citati requisiti, vanno aggiunti:

- l'*autenticazione*, ovvero la capacità del sistema di assicurare al destinatario di un messaggio digitale o di un documento elettronico la corretta identificazione della fonte di provenienza, ovvero la certezza dell'autenticità dell'identità dichiarata dal mittente;
- il *non ripudio*, ovvero la capacità del sistema di garantire che né il mittente, né il destinatario di un messaggio possano negarne la trasmissione o la ricezione.
- il *controllo accessi*, ovvero la capacità del sistema di monitorare e limitare l'accesso ai soli utenti autorizzati, attraverso meccanismi di autenticazione e autorizzazione.

Detti obiettivi possono essere raggiunti attraverso l'implementazione di specifici meccanismi di protezione atti a soddisfare una serie di requisiti funzionali di sicurezza che si distinguono in:

- funzioni di sicurezza fisica*:*
  - *Sistemi di Rilevazione Passiva*: funzioni di sicurezza che rilevano la presenza di situazioni logistiche anomale (ad es. incendio, allagamento, fumo), inviando uno specifico allarme ai centri di controllo senza attivare contromisure;
  - *Sistemi di Rilevazione Attiva*: funzioni di sicurezza che rilevano la presenza di situazioni logistiche anomale (ad es. incendio, allagamento, fumo), inviando uno specifico allarme ai centri di controllo ed attivando una specifica contromisura.
  - *Sistemi di Controllo Accesso Fisico*: funzioni di sicurezza che regolano l'accesso fisico in determinate aree riservate alle sole persone e mezzi autorizzati.
  - *Sistemi di Continuità di Alimentazione*: funzioni di sicurezza che garantiscono la continuità dell'alimentazione elettrica ai sistemi informatici, almeno per il tempo sufficiente alla chiusura ordinata.
  - *Infrastrutture*: accorgimenti specifici sugli edifici e disposizione dei locali al fine di garantire la sicurezza degli impianti (edifici antisismici, uscite di sicurezza dotate di sistemi di allarme, separazione ambienti a rischio, ecc…).
- funzioni di sicurezza logica[6]:
  - *Access Control:* funzioni di sicurezza che controllano il flusso delle informazioni tra processi e dell'utilizzo delle risorse da parte dei processi stessi, con l'obiettivo di assicurare solo agli utenti autorizzati l'espletamento delle operazioni di propria competenza. Tra tali funzioni vanno previste anche quelle di amministrazione dei diritti di accesso e loro verifica.
  - *Accounting:* funzioni di sicurezza che registrano e tracciano le azioni poste in essere da utenti o conseguenti all'esecuzione di processi, con l'obiettivo di assicurarne l'univoca ed incontestabile attribuzione.
  - *Accuracy:* funzioni di sicurezza che garantiscono il mantenimento delle corrette relazioni tra i dati e la non alterazione degli stessi in fase di trasferimento tra i diversi processi. Hanno lo scopo di identificare, segnalare e correggere

[6] Riferimento alla classificazione riportata nello standard ITSEC - Information Technology Security Evaluation Creteria

qualunque tipo di modifica non autorizzata dei dati (alterazioni, cancellazioni ed inclusioni di nuove parti nei dati scambiati tra processi o passati da un oggetto all'altro). Tra queste rientrano anche quelle di identificazione ed eliminazione di Virus, nonché di analisi dell'integrità degli indici di un Data Base.

- *Audit:* funzioni di sicurezza che registrano ed analizzano gli scostamenti, da soglie predeterminate, di determinati eventi che potrebbero rappresentare una minaccia alla sicurezza delle risorse. Hanno l'obiettivo di monitorare e controllare casi anomali o sospetti. Tali funzioni devono consentire l'identificazione selettiva e la correlazione delle azioni eseguite da uno o più utenti, e consentire l'Alert on-line o differito al superamento di soglie di sicurezza predefinite.
- *Data Exchange:* funzioni di sicurezza che garantiscono la protezione dei dati durante la loro trasmissione sui canali di comunicazione mediante l'autenticazione del mittente, l'integrità e la riservatezza del contenuto del messaggio, il non ripudio del mittente e del destinatario.
- *Identification e Authentication:* funzioni di sicurezza che verificano l'identità degli utenti che accedono a risorse controllate. L'identificazione e l'autenticazione devono essere effettuate prima di ogni ulteriore interazione tra l'utente e il sistema. Solo se l'operazione di identificazione e autenticazione sarà andata a buon fine, l'utente autorizzato potrà avere altre interazioni con il sistema. Tali funzioni si applicano anche alle interazioni tra processi applicativi e tra sistemi.
- *Object Reuse:* funzioni di sicurezza che consentono il riutilizzo di spazi di memoria centrale o di massa, impedendo che ciò costituisca una minaccia alla riservatezza delle informazioni precedentemente registrate su tali supporti. Tra queste, anche quelle di inizializzazione e cancellazione dei supporti asportabili e riusabili (ad es. nastri magnetici, dischetti, ecc.).
- *Reliability of Service:* funzioni di sicurezza che assicurano l'accesso e l'utilizzo delle risorse esclusivamente a utenti/processi autorizzati entro tempi prefissati.

– funzioni di sicurezza organizzativa.
  - *Ruoli e Responsabilità:* definizione delle figure organizzative coinvolte negli aspetti di gestione della sicurezza, dei loro compiti e delle relative responsabilità.
  - *Procedure di Gestione:* strutturazione di un sistema documentale rivolto agli addetti alla gestione della sicurezza informatica atto a descrivere le modalità operative di svolgimento delle attività di competenza.
  - *Procedure di Utilizzo:* strutturazione di un sistema documentale rivolto agli utenti dei sistemi informatici atto a descrivere le norme comportamentali e le modalità operative di utilizzo sicuro delle risorse informatiche.
  - *Formazione e Comunicazione:* pianificazione di attività finalizzate alla diffusione di conoscenze e competenze volte a migliorare i comportamenti organizzativi ed operativi degli addetti e degli utenti che operano sulle risorse informatiche.

I meccanismi di protezione, in grado di attuare le funzioni di sicurezza sopra descritte, consistono in misure di sicurezza fisica (ad es. sistemi/apparecchiature), logica (ad es. soluzioni tecnologiche), ed organizzativa (ad es. procedure, istruzioni operative, training, etc..) la cui selezione deve essere effettuata in relazione ai rischi cui le informazioni sono potenzialmente esposte.

Tutte le più accreditate metodologie internazionali di gestione della sicurezza informatica sono concordi quindi nel considerare l'attività di analisi dei rischi come prerequisito per una progettazione razionale dei sistemi di protezione.
Le metodiche e gli strumenti di analisi dei rischi disponibili, anche limitando l'analisi a quelli applicabili in ambito ICT, sono numerosi ma poggiano tutti sui concetti di rischio, di minaccia e di vulnerabilità, danno e impatto.
Il *Rischio* può essere considerato come la probabilità che delle minacce, sfruttando vulnerabilità intrinseche o estrinseche ai beni dell'organizzazione, ovvero agli *asset* (informazioni, risorse hardware, risorse software, location, personale), producano impatti negativi sull'organizzazione, in termini di perdite economiche, violazione normative, rallentamenti dell'operatività, perdita di immagine etc...
La *Minaccia* viene generalmente definita come un evento od una azione, di natura accidentale o deliberata, che, sfruttando punti deboli o vulnerabilità del sistema, delle applicazioni o dei servizi, risulta potenzialmente idonea a provocare effetti dannosi sull'organizzazione. Le minacce possono essere raggruppate in:

- minacce fisiche: sono quelle che insistono sulle aree, sugli edifici, sui locali, sugli uffici e che sfruttano le vulnerabilità in ambiente fisico. Tali minacce si riferiscono agli asset di tipo hardware ed alle location ;
- minacce tecnologiche: sono quelle che insistono sull'architettura e sui sistemi e che sfruttano le vulnerabilità delle configurazioni o delle installazioni. Tali minacce si riferiscono agli asset di tipo hardware e software;
- minacce organizzative: sono quelle che sfruttano le vulnerabilità rappresentate dal mancato senso di appartenenza, responsabilità e professionalità da parte del personale.

Infine, la *Vulnerabilità* è una condizione di debolezza nel sistema operativo, nelle procedure di sicurezza, nei controlli interni (tecnici, operazionali e/o gestionali) o nella loro implementazione che, se sfruttata da una minaccia, può compromettere la riservatezza, l'integrità e la disponibilità dei beni aziendali.
Le vulnerabilità possono dipendere dalla mancanza di appropriati meccanismi di sicurezza o da deficienze nelle procedure di utilizzo da parte degli utenti, da carenze organizzative o di assegnazione di responsabilità, dalla collocazione geografica del sistema informatico (es. ubicazione in una zona altamente sismica), da errori sistemici presenti nell'hardware o nel software (es. errori di progettazione), da possibili malfunzionamenti accidentali dell'hardware.
Le organizzazioni che intendono affrontare in maniera adeguata ed efficace il problema della sicurezza informatica devono creare adeguati programmi di gestione delle minacce e delle vulnerabilità, in modo da tenere sotto controllo i rischi, reagire prontamente ad ogni specifico problema e risolvere rapidamente tutti gli incidenti quando si verificano.
Il *Danno* è la conseguenza negativa del verificarsi di un rischio o dell'attuarsi di una minaccia. Tali conseguenze vengono spesso identificate da una perdita di riservatezza, integrità e/o disponibilità dell'informazione.
In alcuni casi, questa definizione condivisa viene però ulteriormente specificata. Ad esempio si può distinguere il danno in "tangibile" (danno monetario provocato sul sistema) e "intangibile"

(danno di immagine o comunque immateriale)[7], oppure in "business consequence" (frodi o attacchi informatici andati a buon fine) e "security breach" (perdita di disponibilità, integrità, riservatezza dovuti ad un incidente, come un guasto agli elaboratori).
L'*Impatto* è un concetto presente nella maggior parte degli strumenti/metodologie di analisi dei rischi la cui definizione spesso si sovrappone a quella di danno.
Alcuni strumenti/metodologie associano il concetto di impatto a quello di misura o entità del danno, ma la definizione che accomuna la maggior parte di essi[8] vede l'impatto come effetto sull'azienda o ente e sul suo business del verificarsi di una minaccia, quindi l'effetto reale del danno sul sistema. L'impatto in questa accezione deve tenere conto ad esempio anche di possibili responsabilità civili o penali (presenti ad esempio nel D. Lgs. 196/2003).

3. Quadro normativo nazionale di riferimento

Ai fini dell'individuazione del quadro normativo nazionale di riferimento, assumono rilevanza gli obiettivi che attraverso la sicurezza informatica si intendono raggiungere.
La sicurezza informatica ha come obiettivo principale quello di garantire, mediante l'adozione di misure di sicurezza, un adeguato grado di protezione delle informazioni e delle risorse dell'organizzazione sia da minacce provenienti dall'interno (es. abusi di privilegi, utilizzo a fini personali delle risorse aziendali, diffusione di virus informatici, frodi informatiche, etc..) che dall'esterno (es. intrusioni da parte di hacker, introduzione di virus informatici, frodi informatiche, sabotaggi, spionaggio, modifica o cancellazione di dati/informazioni, attentati a sistemi informatici che supportano l'erogazione di servizi di pubblica utilità, etc..).
La Commissione delle Comunità Europee ha qualificato alcuni dei comportamenti che costituiscono una minaccia alla sicurezza informatica, come condotte giuridicamente perseguibili dalle legislazioni degli Stati Membri. Al riguardo, nella **Comunicazione del 26 gennaio 2001**, la Commissione ha operato una distinzione tra "reati informatici specifici" e "reati di tipo convenzionale" perpetrati con l'ausilio delle tecnologie informatiche.[9]
Relativamente ai reati specificamente informatici la Commissione delle Comunità Europee ha evidenziato come sia a livello di Unione europea che di Stati membri siano stati regolamentati sulla base della seguente classificazione :

- **Reati contro la riservatezza**. "…numerosi paesi hanno introdotto norme penali che affrontano gli illeciti attinenti la raccolta, la memorizzazione, l'alterazione, la divulgazione e diffusione di dati personali. A livello di Unione europea, sono state adottate due direttive

---

[7] "Security impacts can be tangible, such as fines, or intangible, like loss of reputation. Impact is defined as a consequence of an undesirable incident that can be caused deliberately or accidentally and affects the software. The consequences can result in destruction or damage of software artifacts or even in loss of confidentiality, integrity, or availability" (Standard ISO/IEC 21827).

[8] ISA, CRAMM, EBIOS, ISO21827, OCTAVE, RAF, SARA, SPRINT e CETRA

[9] Capitolo 3 della Comunicazione della Commissione al Consiglio, al Parlamento europeo, al Comitato economico e sociale e al Comitato delle Regioni Bruxelles - "Creare una società dell'informazione sicura migliorando la sicurezza delle infrastrutture dell'informazione e mediante la lotta alla criminalità informatica". Bruxelles 30 gennaio 2001 - COM(2000) 890.

che ravvicinano le disposizioni nazionali in materia di tutela della riservatezza con riguardo al trattamento dei dati personali...".[10]

- **Reati relativi ai contenuti**. "…la diffusione, soprattutto mediante Internet, della pornografia, e in particolare della pornografia infantile, di affermazioni razziste e di informazioni che incitano alla violenza inducono a chiedersi in quale misura tali atti possano essere affrontati con l'ausilio del diritto penale. La Commissione ha sostenuto la tesi che ciò che è illecito off-line dovrebbe essere tale anche on-line. L'autore o il fornitore dei contenuti può essere chiamato a rispondere in sede penale. È stata adottata una decisione del Consiglio per combattere la pornografia infantile su Internet……." [11]
- **Reati contro il patrimonio, accesso non autorizzato e sabotaggio**. "… numerosi paesi hanno introdotto norme relative ai reati contro il patrimonio specificamente connessi agli strumenti informatici e definiscono nuove fattispecie legate all'accesso non autorizzato ai sistemi informatici (ad esempio, la pirateria, il sabotaggio di elaboratori e la diffusione di virus informatici, lo spionaggio informatico, la falsificazione informatica e la frode informatica) e nuove modalità di violazione (ad esempio, manipolazioni di elaboratori invece di inganni a danno di individui). L'oggetto del reato è spesso immateriale, ad esempio, denaro in depositi bancari o programmi informatici…."
- **Reati contro la proprietà intellettuale**. "…sono state adottate due direttive, relative alla tutela giuridica dei programmi per elaboratore e delle banche dati che trattano direttamente di temi inerenti alla società dell'informazione e prevedono l'adozione di sanzioni. Il Consiglio ha adottato una posizione comune concernente una proposta di direttiva sul diritto d'autore e sui diritti connessi nella società dell'informazione….E' necessario reprimere la violazione del diritto d'autore e dei diritti connessi, così come l'elusione delle misure tecnologiche volte a tutelare tali diritti…" .[12]

In conformità alle indicazioni fornite dalla Comunità Europea e agli orientamenti della legislazione nazionale, rilevano nell'ambito della gestione della sicurezza informatica le normative, a carattere generale, riportate di seguito in ordine cronologico:

- Deliberazione n.45 del 21 Maggio 2009 – "Regole per il riconoscimento e la verifica del documento informatico"
- D.P.C.M. 30 marzo 2009 - "Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici".
- Legge 18 marzo 2008, n. 48 "Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno".

---

[10] La Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, è relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati. La Direttiva 97/66/CE del Parlamento europeo e del Consiglio, del 15 dicembre 1997, è relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle telecomunicazioni.

[11] Decisione del Consiglio, del 29 maggio 2000, relativa alla lotta contro la pornografia infantile su Internet (GU L 138 del 9.6.2000, pag.1).

[12] Direttiva 91/250/CEE del Consiglio, del 14 maggio 1991, relativa alla tutela giuridica dei programmi per elaboratore (GU L 122 del 17.5.1991, pagg. 42 – 46). Direttiva 96/9/CE del Parlamento europeo e del Consiglio, dell'11 marzo 1996, relativa alla tutela giuridica delle banche di dati (GU L 77 del 27.3.1996, pagg. 20 – 28).

- Legge 6 febbraio 2006 n.38 - " "Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet".
- Decreto legislativo 30 giugno 2003, n.196 - "Codice in materia di protezione dei dati personali"
- Legge 23 dicembre 1993 n.547 - "Modificazioni e integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica" (cd. Legge sui Reati informatici).
- Legge 22 aprile 1941 n.633 - "Protezione del diritto d'autore e di altri diritti connessi al suo esercizio"– testo coordinato con successive modifiche e integrazioni .

Particolare rilievo tra le normative sopra citate assume il **D.Lgs.196/2003** poiché nell'ambito della tutela dei dati personali[13] prevede una serie di obblighi generali e specifici di sicurezza introducendo il concetto giuridico di "rischio", di "misura idonea" e di "misura minima".

In via generale, il decreto stabilisce all'art. 31[14] che devono essere individuate idonee e preventive misure di sicurezza al fine di proteggere i dati dai rischi di distruzione (riconducibile agli obiettivi di sicurezza della disponibilità e dell'integrità), perdita (riconducibile all'obiettivo di sicurezza della disponibilità) e accesso non autorizzato (riconducibile agli obiettivi di sicurezza della confidenzialità, disponibilità ed integrità), trattamento non conforme o non consentito (riconducibile al controllo accessi e all'integrità dei programmi).

Le misure minime (artt. 33, 34, 35) garantiscono invece quello che la legge definisce il "livello minimo" di protezione dei dati e la loro adozione è "conditio sine qua non" per lo svolgimento delle attività di trattamento. Dette misure devono essere implementate secondo le modalità definite nel Disciplinare Tecnico allegato al Codice (Allegato B), si applicano sia ai trattamenti effettuati nel settore privato che in quello pubblico, e sono individuate rispettivamente per:

- Trattamenti svolti con l'ausilio di strumenti elettronici (art. 34 del D.Lgs. 196/03):
  - utilizzo di un sistema di autenticazione informatica;
  - adozione di procedure di gestione delle credenziali di autenticazione ed utilizzo di un sistema di autorizzazione;
  - aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
  - protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti, ad accessi non autorizzati ed a determinati programmi informatici;
  - adozione di procedure per la custodia di copie di sicurezza, e per il ripristino

---

[13] Art.4 1c lett.b) del D.Lgs.196/2003 "dato personale, qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale".

[14] Art.31 del D.Lgs.196/2003 – "Obblighi di sicurezza – I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalita' della raccolta".

della disponibilità dei dati e dei sistemi;
    - tenuta di un aggiornato Documento Programmatico sulla Sicurezza nel caso di trattamento di dati sensibili e/o giudiziari;
    - adozione di tecniche di cifratura o di codici identificativi per dati idonei a rivelare lo stato di salute o la vita sessuale, trattati da organismi sanitari;
- Trattamenti svolti senza l'ausilio di strumenti (art. 35 del D.Lgs. 196/03):
    - aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;
    - previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;
    - ed infine, previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.

Le conseguenze giuridiche derivanti dalla mancata identificazione e implementazione delle misure idonee di sicurezza sono diverse da quelle connesse all'omessa attuazione delle misure minime. Per le prime è prevista, nel caso di danno a terzi, una responsabilità oggettiva ex art. 2050 del cod. civ., mentre per le seconde l'applicazione di una sanzione penale (art. 169 del D.Lgs. 196/03) consistente nell'arresto fino a 2 anni o nel pagamento di una somma da 10.000 a 50.000 euro.

L'attuazione delle misure di sicurezza risulta fondamentale anche nell'ambito di alcune tutele previste dalla **Legge 547/93.** Al riguardo, la legge tutela i sistemi dotati di misure di sicurezza tecnologiche e/o organizzative che esprimono la volontà di riservare l'accesso, la permanenza o l'utilizzo delle risorse informative al solo personale autorizzato (Sentenza 21 aprile 2000 n. 6677/99 R.G.G.I.P., del Tribunale Penale di Roma, Ufficio GIP, Sezione 8a). La predisposizione delle misure di sicurezza da parte dell'organizzazione, quindi:

- è necessaria per la punibilità di alcuni comportamenti;
- manifesta la volontà dell'organizzazione di riservare l'accesso o la permanenza solo alle persone autorizzate;
- garantisce l'organizzazione, e coloro che ne hanno la responsabilità, dai rischi di coinvolgimento sia patrimoniale che penale per i fatti penalmente rilevanti tenuti da dipendenti o da terzi.

Alla luce delle disposizioni in materia di obblighi generali e specifici di sicurezza previste dal D.Lgs. 196/2003, è facile identificare queste misure con quelle previste dal sopra citato decreto agli artt. 31, 33, 34, 35 ed all'Allegato B, quando il reato informatico riguarda informazioni, documenti, sistemi e comunicazioni contenenti e/o riguardanti dati personali.

Accanto al quadro giuridico generale sopra menzionato, è opportuno ricordare anche alcune normative e Best Practice nazionali di riferimento nell'ambito delle pubbliche amministrazioni. In particolare:

- Linee Guida AIPA 28 ottobre 1999 – Definizione di un piano per la sicurezza;
- Decreto MI 19 luglio 2000 - Regole tecniche e di sicurezza per carta d'identità e documento d'identità elettronici;
- D.P.C.M. 31 ottobre 2000 - Regole tecniche per il protocollo informatico;
- D.P.R. n 445 del 28 dicembre 2000 – T.U. in materia di documentazione amministrativa.

- Raccomandazione n. 1/2000 - AIPA - Sicurezza dei siti web delle PA;
- Linee Guida AIPA 20 settembre 2001 - Manuale dei livelli di servizio nel settore ICT;
- Linee Guida AIPA 4 novembre 2001 - Sicurezza dei servizi in rete;
- D.P.C.M. 16 gennaio 02 - Sicurezza Informatica e delle Telecomunicazioni nelle P.A;
- Direttiva del MIT 11 giugno 2002 - Linee guida del Governo per lo sviluppo della Società dell'Informazione;
- Direttiva del MIT 20 dicembre 2002 - Linee guida in materia di digitalizzazione dell'Amministrazione;
- Decreto 9 dicembre 2004 – Regole tecniche di sicurezza relative alle tecnologie ed ai materiali utilizzati per la produzione della carta nazionale dei servizi;
- Deliberazione AIPA 11/2004 - Regole tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformità dei documenti agli originali;
- Linee Guida del Comitato tecnico nazionale sulla sicurezza informatica e delle comunicazioni nelle pubbliche amministrazioni - "Proposte concernenti le strategie in materia di sicurezza informatica e delle telecomunicazioni per la pubblica amministrazione" (marzo 2004).

Tra le normative e le linee guida emanate per la pubblica amministrazione, ma di riferimento anche per il settore privato, assumono particolare rilievo il **D.P.C.M. del 16 gennaio del 2002** emanato dal Dipartimento per l'Innovazione e le Tecnologie (MIT) ed il documento "**Proposte concernenti le strategie in materia di sicurezza informatica e delle telecomunicazioni per la pubblica amministrazione**" (**marzo 2004**), emanato dal Comitato tecnico nazionale sulla sicurezza informatica e delle comunicazioni nelle pubbliche amministrazioni in ossequio all'articolo 2, comma 1 del decreto istitutivo del Comitato stesso.

La Direttiva afferma che "…le informazioni gestite dai sistemi informativi pubblici costituiscono una risorsa di valore strategico per il governo del paese".

Questo patrimonio, dunque, deve essere adeguatamente protetto e tutelato al fine di prevenire possibili alterazioni sul significato delle informazioni stesse.

"…E' noto infatti che esistono minacce di intrusione e possibilità di divulgazione non autorizzata di informazioni, nonché di interruzione e di distruzione del servizio….", ed assume "…importanza fondamentale valutare il rischio connesso con la gestione delle informazione e dei sistemi.".

La Direttiva stabilisce i criteri per una prima autovalutazione sul grado di sicurezza tecnologica di ogni amministrazione al fine di poter definire il proprio livello di rischio, raccomandando alle stesse di agire con la massima priorità ed urgenza.

Le Pubbliche Amministrazioni devono, dunque, essere in grado di garantire l'integrità e l'affidabilità dell'informazione pubblica attraverso quelle che la direttiva stessa definisce "….credenziali di sicurezza conformi agli Standard Internazionali di riferimento".

Con tale affermazione, la Direttiva riconosce negli Standard Internazionali di riferimento in materia di gestione della sicurezza (attualmente l'ISO/IEC 27002), lo strumento maggiormente idoneo per affrontare e gestire efficacemente la problematica.

Il Comitato tecnico nazionale sulla sicurezza informatica e delle comunicazioni nelle pubbliche amministrazioni nella proposta del marzo 2004, nell'ambito della certificazione

ICT, promuove il ricorso agli Standard di sicurezza riconosciuti a livello internazionale, che "…rappresentano un mezzo importante per costruire la fiducia e la confidenza sia nei confronti di un'organizzazione che tra le varie parti coinvolte…". In particolare la proposta fa riferimento a due standard ISO/IEC:

- Lo standard ISO 15408, noto anche come Common Criteria for Information Technology Security, che "...fornisce le principali direttive per la valutazione e certificazione di prodotti e sistemi informatici".
- Lo standard ISO 17799 (oggi ISO/IEC 27002), che "...fornisce importanti indicazioni sulle misure organizzative da intraprendere, in un'azienda, per poter far fronte al problema della sicurezza informatica".

4. La posizione dell'Unione Europea

Il problema della sicurezza informatica è diventata una fonte di preoccupazione crescente per la società moderna ed è stato oggetto di attente analisi da parte dell'Unione Europea.
La Commissione Europea nella **Comunicazione del 26 gennaio del 2001**[15] al Consiglio, al Parlamento europeo, al Comitato economico e sociale e al Comitato delle regioni ribadisce che "…. le infrastrutture dell'informazione e delle comunicazioni, elemento critico delle nostre economie, presentano dei punti vulnerabili e offrono nuove possibilità di comportamenti criminali, che possono assumere una grande varietà di forme e avere una portata transnazionale. Sebbene, per diversi motivi, manchino dati statistici attendibili, non vi è dubbio che i reati informatici costituiscono una minaccia per gli investimenti e le attività degli operatori del settore, nonché per la sicurezza e la fiducia nella società dell'informazione. ….È possibile agire per prevenire le attività criminali sia aumentando la sicurezza delle infrastrutture dell'informazione sia facendo in modo che le autorità preposte all'applicazione della legge dispongano di opportuni strumenti d'intervento, nel pieno rispetto dei diritti fondamentali dei cittadini."
La strategia di gestione della sicurezza proposta dalla Commissione Europea già a partire dal 2001 comprendeva misure volte a:

- proteggere gli elementi critici dell'infrastruttura, mediante l'impiego di infrastrutture a chiave privata (PKI), lo sviluppo di protocolli sicuri, ecc.
- proteggere gli ambienti privati e pubblici mediante lo sviluppo di software di qualità, di 'firewall', programmi antivirus, sistemi di gestione dei diritti elettronici, crittazione, ecc.
- rendere sicura l'autenticazione degli utenti autorizzati, l'uso delle carte intelligenti, l'identificazione biometrica, le firme digitali, le tecnologie basate su ruoli, ecc.

In quest'ottica, la Commissione nella successiva **Comunicazione del 6 giugno del 2001**[16],

---

[15] *Comunicazione del 26 gennaio del 2001* della Commissione al Consiglio, al Parlamento europeo, al Comitato economico e sociale e al Comitato delle regioni "Creare una società dell'informazione sicura migliorando la sicurezza delle infrastrutture dell'informazione e mediante la lotta alla criminalità informatica"

[16] *Comunicazione del 6 giugno del 2001*, presentata dalla Commissione delle Comunità Europee al Parlamento europeo, al Consiglio, al Comitato economico e sociale e al comitato delle regioni avente ad oggetto il tema della "Sicurezza delle

specifica che con la locuzione "sicurezza delle reti e dell'informazione" si deve intendere la "… capacità di una rete o di un sistema d'informazione di resistere, ad un determinato livello di riservatezza, ad eventi imprevisti o atti dolosi che compromettono la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati conservati o trasmessi e dei servizi forniti o accessibili tramite la suddetta rete o sistema….".

Il Consiglio dell'Unone Europea nella **Risoluzione del 28 gennaio del 2002**[17] ha ulteriormente specificato che la sicurezza delle reti e dell'informazione consiste nell'assicurare la disponibilità di servizi e di dati:

- impedendo interruzioni o intercettazioni abusive delle comunicazioni;
- confermando che i dati trasmessi, ricevuti o archiviati sono completi e invariati;
- assicurando la riservatezza dei dati e proteggendo i sistemi da accessi non autorizzato e software maligni;
- garantendo, infine, l'affidabilità dell'autenticazione.

Il Consiglio dell'Unone Europea ha affermato inoltre che gli Stati membri "…. devono promuovere l'applicazione delle migliori pratiche in materia di sicurezza basate su dispositivi vigenti quali l'ISO/IEC 17799…"

Quindi, secondo l'orientamento comunitario al fine di assicurare la corretta gestione del problema della sicurezza delle reti e dell'informazione, è necessaria la strutturazione di un Information Security Management System (ISMS) conforme allo Standard Internazionale ISO/IEC 27002 (ex ISO/IEC 17799).

Al fine di supportare gli Stati Membri nella lotta alla criminalità informatica il Parlamento Europeo e il Consiglio dell'Unione Euroepa hanno istituito[18] l'Agenzia europea per la sicurezza delle reti e dell'informazione (**ENISA**) con il compito di svolgere una funzione consultiva e di coordinamento delle misure adottate dalla Commissione e dai paesi dell'Unone Europea per rendere più sicure le loro reti e i loro sistemi di informazione.

Sempre con l'obiettivo di combattere la criminalità informatica, promuovere la sicurezza dell'informazione e rafforzare la cooperazione tra le autorità giudiziarie e le altre autorità competenti, il Consiglio dell'Unione Euroepa ha promosso[19] un ravvicinamento delle legislazioni penali e una repressione degli attacchi ai sistemi informatici per quanto riguarda l'accesso illecito ai sistemi, l'attentato all'integrità di un sistema e l'attentato all'integrità dei dati.

Con la **Comunicazione del 31 maggio del 2006**[20] l'Unione Europea ha dato nuovo impulso alla strategia della Commissione europea definita nella Comunicazione del 2001 "Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo", affermando che " …per individuare e rispondere alle sfide alla sicurezza dei sistemi informatici e delle reti

reti e sicurezza dell'informazione: proposta di un approccio strategico europeo.

[17] *Risoluzione del 28 gennaio del 2002 del Consiglio dell'Unine Europea* "Approccio comune e ad azioni specifiche nel settore della sicurezza delle reti 2002/C43/02".

[18] Regolamento (CE) n. 460/2004 del 10 marzo 2004

[19] Decisione Quadro 2005/222/GAI del 24 febbraio 2005

[20] Bruxelles, 31.5.2006 COM(2006) 251. Comunicazione della Commissione al Consiglio, al Parlamento Europeo, al Comitato Economico e Sociale Europeo e al Comitato Delle Regioni - "Una strategia per una società dell'informazione sicura. Dialogo, partenariato e responsabilizzazione"

nell'Unione Europea è necessario il pieno impegno di tutte le parti interessate ....” non solo, quindi, gli Stati membri ma anche tutti gli attori del settore privato.
Nella Comunicazione si precisa inoltre che “…La Commissione intende chiedere all'ENISA di sviluppare un partenariato di fiducia con gli Stati membri e le parti interessate al fine di sviluppare un quadro adeguato per la raccolta di dati, con meccanismi e procedure per la raccolta e l'analisi di dati sugli incidenti a danno della sicurezza e sulla fiducia dei consumatori a livello comunitario”.

5. Il contesto internazionale: Gli Standard di sicurezza

Gli standard internazionali dell'Information Security sono documenti di riferimento emessi da enti normativi nazionali (come ad es. il British Standard Institute - BSI) o internazionali (come ad es. l'ISO) nati in risposta alla precisa domanda dei settori dell'industria, del commercio e delle amministrazioni statali, di definire un framework comune per valutare il livello di affidabilità di un sistema/prodotto ICT, e sviluppare ed implementare sistemi di gestione della sicurezza delle informazioni[21].
Dunque, a seconda degli obiettivi da conseguire il contenuto degli Standard può riguardare principalmente le seguenti aree tematiche:

- Tecnologie informatiche utilizzate per la difesa del patrimonio informatico:
  - lo Standard TCSEC (1985);
  - lo Standard ITSEC (1991);
  - lo Standard ISO/IEC 15408 (1999);

[21] Nel documento “Proposte concernenti le strategie in materia di sicurezza informatica e delle telecomunicazioni per la pubblica amministrazione” (marzo 2004) il Comitato tecnico nazionale sulla sicurezza informatica e delle comunicazioni nelle pubbliche amministrazioni ha riconosciuto negli attuali Standard Internazionali gli strumenti per la certificazione della sicurezza ICT. All'interno della proposta si scrive “… nel 1999 è stata adottata in tutte le sue tre parti dall'ISO/IEC la raccolta di criteri denominata Common Criteria che consente la valutazione e certificazione della sicurezza di prodotti e sistemi ICT. Tale adozione si è formalmente realizzata attraverso l'emanazione dello standard ISO/IEC IS 15408. L'anno successivo, questo stesso organismo internazionale ha fatto propria la prima parte di un altro standard di certificazione della sicurezza ICT sviluppato in Gran Bretagna, il ben noto BS7799 che nella versione ISO/IEC ha assunto prima la denominazione ISO/IEC 17799 e poi nel 2007 quella di ISO/IEC 27002. La seconda parte dello standard, quella che contiene le indicazioni più precise ai fini della certificazione, è invece divenuta ISO nel 2005 con la denominazione ISO/IEC 27001. Lo standard ISO/IEC IS 15408 (Common Criteria) e lo standard ISO/IEC 27001, sebbene abbiano in comune la sicurezza ICT, hanno lo scopo di certificare cose ben diverse. Nel caso dei Common Criteria (in seguito denominati brevemente CC), infatti, oggetto della certificazione è, come già anticipato, un sistema o un prodotto ICT13, nel caso invece dell'ISO/IEC 27001 ciò che viene certificato è il processo utilizzato da un'organizzazione, sia essa una società privata o una struttura pubblica, per gestire al suo interno la sicurezza ICT (tale processo, come è noto, viene indicato nello standard con l'acronimo ISMS che sta per “Information Security Management System”). In altri termini, la certificazione ISO/IEC 27001 può essere considerata una certificazione aziendale, del tipo quindi della ben nota certificazione ISO 9000, ma specializzata nel campo della sicurezza ICT.

- Organizzazione e gestione della sicurezza:
    - Lo Standard ISO/IEC 27001:2005 "Standard for ISMS";
    - lo Standard ISO/IEC 27002:2007 "Code of Practice for ISMS";
    - lo Standard ISO/IEC 27005:2008 "Standard for Information risk and management";
    - La serie ISO/IEC TR 13335.

Lo **Standard ITSEC** (*Information Technology Security Evaluation Criteria*) nasce nel 1991 come evoluzione dello Standard TCSEC più noto come "Orange Book"[22], e con l'obiettivo di fornire un framework per la valutazione e la certificazione delle funzionalità di sicurezza (tecniche e non tecniche) di:

- un sistema informatico, ossia una specifica installazione IT avente uno preciso scopo in un ambiente operativo completamente definito;
- un prodotto informatico, ossia un dispositivo hardware o un pacchetto software progettati per l'uso e l'installazione in una grande varietà di sistemi.

Nonostante le evidenti differenze tra sistemi e prodotti, lo Standard ITSEC prevede che entrambi siano valutati secondo gli stessi criteri, e che vengano al riguardo identificati dal termine TOE (*Target of Evaluation*). Il TOE, in ITSEC è dunque, l'oggetto della valutazione.
La certificazione è effettuata sulla base di un Security Target ovvero di un documento, definito dal committente, nel quale sono specificate le funzioni di sicurezza che devono essere soddisfatte dal TOE e riportate altre informazioni rilevanti, quali gli obiettivi di sicurezza del sistema/prodotto (in termini di riservatezza, integrità e disponibilità).
La descrizione delle funzioni di sicurezza costituisce la parte più importante del Security Target. Al riguardo lo Standard suggerisce l'ordinamento delle funzioni di sicurezza in 8 gruppi generici, "Generic Headings".
Nell'approccio ITSEC, l'operazione di valutazione del livello di sicurezza, intesa come affidabilità del sistema/ prodotto informatico, si pone due obiettivi fondamentali[23]:

- valutare l'efficacia delle funzioni di sicurezza, in termini di capacità del sistema/ prodotto di contrastare efficacemente le minacce alle quali si ritiene sia esposta l'informazione dallo stesso elaborata o immagazzinata;
- valutare la corretta realizzazione delle funzioni di sicurezza e dei corrispondenti meccanismi.

Lo Standard definisce 7 livelli di valutazione dell'affidabilità del sistema/prodotto informatico

---

[22] Il problema della sicurezza dei sistemi operativi fu affrontato per la prima volta in maniera sistematica dal National Computer Security Center (NCSC) usa nella pubblicazione "Trusted Computer System Evaluation Criteria" (TCSEC, nota anche come "Orange Book"). Lo standard introduce i concetti di "politica della sicurezza", intesa come guida formale, esplicita e conosciuta alla esecuzione delle contromisure, di "contromisura" come atto di protezione dei beni adeguato al valore ed al livello di rischio cui gli stessi sono esposti, e stabilisce anche classifica delle contromisure. Dall'Orange Book nel 1991 è stata ricavata una rielaborazione adottata da alcuni paesi europei nota anche come "White Book" il cui nome ufficiale è ITSEC "Information Technology Security Evaluation Criteria". Poiché all'interno dell'Unione europea questo Standard non era l'unico documento adottato dai diversi paesi la CEE redisse nel 1991 un Manuale di riconoscimento delle diverse procedure noto come ITSEM "IT Security Evaluation Manual".

[23] Fonte: documento "Privacy: la sicurezza informatica nell'unione europea ed i criteri ITSEC" (Milano, 1997) del dott. Marco Maglio (reperibile sul sito www.privacy.it).

che rappresentano, dunque, la capacità di quest'ultimo di realizzare le specifiche di sicurezza attraverso le funzioni sopra citate.

Lo Standard **ISO/IEC 15408** (*Common Criteria for information technology security evaluation*), nasce dallo sforzo dei rappresentanti degli Stati Uniti, Canada, Francia, Germania, Olanda e Regno Unito, in collaborazione con l'ISO (International Organization for Standardization) di sviluppare uno standard internazionale di valutazione della sicurezza in ambito informatico.

L'obiettivo era quello di sostituire gli Standard TCSEC e ITSEC attraverso la definizione di nuovi criteri in grado di consentire il reciproco riconoscimento della valutazione dei prodotti di sicurezza.

Nel 1996 fu rilasciata la versione 1.0 dei Common Criteria. Nell'ottobre 1998 si ebbe il rilascio della versione 2.0 (DIS 15408) che, ora con l'approvazione finale dell'ISO è divenuta a tutti gli effetti un International Standard (ISO/IEC 15408). A gennaio 1999 fu rilasciata una versione draft (v 0.6) della Common Evaluation Methodology avente lo scopo di armonizzare le modalità di valutazione da parte degli enti valutatori. Tale metodologia è alla base per il reciproco riconoscimento.[24]

I Common Criteria dunque, delineano regole e direttive comuni per gli sviluppatori e per gli enti di valutazione, e rappresenta una guida ed una fonte di consultazione per gli utenti degli stessi sistemi informatici.

Come per lo Standard ITSEC, il processo di certificazione della sicurezza di un sistema/prodotto informatico previsto dai Common Criteria si pone l'obiettivo di valutare un sistema/prodotto in base all'efficacia delle funzioni di sicurezza garantite ed alla corretta realizzazione delle stesse e dei corrispondenti meccanismi di sicurezza.

I livelli di valutazione previsti dai Common Criteria sono 7, vengono identificati con la sigla EAL (Evaluation Assurance Levels) e sono stati definiti in modo da essere confrontabili con gli equivalenti livelli dei TCSEC e ITSEC:

- EAL1 testato funzionalmente;
- EAL2 testato strutturalmente;
- EAL3 testato e verificato metodicamente;
- EAL4 progettato, testato e riveduto metodicamente;
- EAL5 progettato e testato in modo semi-formale;
- EAL6 verifica del progetto e testing semi-formali;
- EAL7 verifica del progetto e testing formali.

Il sistema dei Common Criteria utilizza i *Protection Profile* per la valutazione del sistema/prodotto informatico. Il Protection Profile è un documento che contiene l'insieme di requisiti di sicurezza, il loro significato e le ragioni per cui sono necessari, oltre che il livello EAL che il sistema/prodotto deve soddisfare. Esso descrive le condizioni ambientali, gli obiettivi ed il livello previsto per la valutazione della funzionalità e della garanzia, specificando le motivazioni delle scelte effettuate circa il grado di garanzia e di robustezza dei meccanismi di protezione. Il Protection profile è, dunque, l'input per il prodotto da valutare (TOE).

L'utilizzo di prodotti certificati, non solo è spesso richiesta dalle normative nazionali, ma offre

---

[24] Fonte: documento "Introduzione ai nuovi standard di sicurezza" dell' Ing. Luigi Baffigo (reperibile sul sito www.privacy.it).

numerosi benefici, tra cui la disponibilità di un documento delle specifiche di sicurezza dei sistema/prodotto (il *Security Target*), contenente sia la descrizione delle minacce che il prodotto è in grado di contrastare, sia l'esistenza di test e di verifiche effettuate, secondo metodologie documentate, da un ente indipendente.
Inoltre, oggigiorno le pubblicazioni relative ai Common Criteria rappresentano un valido strumento di supporto nelle attività di progettazione di infrastrutture di sicurezza informatica, ancorché non s'intenda sottoporle al processo di certificazione.
Lo **standarad ISO/IEC 27001:2005** *(Standard for information security management systems)* è uno standard di Sicurezza delle Informazioni che deriva dallo standard BS 7799 sviluppato dal britannico British Standard Institute (BSI).
Il documento originario (la cui prima edizione venne rilasciata nel 1995 mentre la seconda nel 1999) si componeva di due parti: Parte 1 - BS 7799-1:1999 "Code of practice for information security management"; Parte 2 - BS 7799-2:1999 "Specification for information security management system".
La Parte 1 forniva delle indicazioni, ovvero dei suggerimenti non prescrittivi per proteggere il patrimonio informativo di un organizzazione, mentre la Parte 2 forniva (e fornisce ancora) le prescrizioni da seguire per il conseguimento della certificazione di sicurezza.
Successivamente, l'ISO ha adottato lo standard BS7799 come proprio mediante una procedura non usuale (ancorché prevista dai regolamenti dell'ISO stessa) consistente nella dichiarazione formale che lo standard, così com'era, era da considerarsi approvato e sottoscritto dall'ISO[25].
Attualmente, a seguito di alcune evoluzioni nei contenuti sia della 1° che della 2° parte, la parte 2 nel 2005 è divenuta ISO/IEC 27001 e la parte 1 nel 2007 è divenuta ISO/IEC 27002.
Oggi, come all'origine la ISO/IEC 27001 costituisce lo schema di riferimento per il conseguimento della certificazione di sicurezza. Oggetto della valutazione è il processo utilizzato dall'organizzazione (indicato nello standard con l'acronimo ISMS che sta per "Information Security Management System"), sia essa una società privata o una struttura pubblica, per gestire al suo interno la sicurezza ICT [26].
Lo schema di certificazione presentato dalla ISO/IEC 27001, prevede l'approntamento da parte dell'organizzazione delle seguenti attività:

- Impostazione del processo di gestione della sicurezza delle informazioni, ovvero definizione delle fasi e delle attività dell'ISMS (Management Framework);
- Implementazione ed Operatività dell'ISMS;
- Monitoraggio e revisione dell'ISMS;
- Mantenimento e accrescimento dell'ISMS;
- Predisposizione del sistema documentale (Politiche di sicurezza, Valutazione e Gestione del rischio, Procedure operative dell'ISMS, Registrazioni, Statement of Applicability);
- Gestione controllata della documentazione.

---

[25] Fonte: White Paper "Introduzione agli standard di Sicurezza delle Informazioni ed Informatica" di Alessandro Bottonelli.

[26] In altri termini, la certificazione ISO/IEC 27001 può essere considerata una certificazione aziendale, assimilabile alla ben nota certificazione ISO 9000, ma specializzata nel campo della sicurezza ICT.

Per quanto attiene l'identificazione degli obiettivi di controllo e dei controlli da attuare nell'ambito dell'ISMS, lo Standard ISO/IEC 27001 propone 11 aree tematiche più specificatamente dettagliate dalla ISO/IEC 27002. I controlli presenti al'interno delle aree tematiche, consistono in pratiche, procedure o meccanismi in grado di gestire i rischi, attraverso la riduzione delle minacce e delle vulnerabilità, la limitazione dei possibili impatti e la trattazione degli eventi critici (reazione e ripristino in tempi brevi delle condizioni iniziali).
Lo standarad **ISO/IEC 27002:2007** (*Code of practice for information security management*) fornisce le linee guida per la creazione di un sistema di gestione della sicurezza delle informazioni certificabile, prendendo in considerazione i più recenti sviluppi nell'applicazione dell'Information Processing Technology.
In particolare, l'ISO/IEC 27002:

- costituisce un framework di riferimento a livello internazionale, ovvero un insieme di principi e di linee guida, per la strutturazione di un Sistema di Gestione della Sicurezza delle Informazioni (*Information Security Management System* - ISMS);
- fornisce agli addetti ai lavori una metodologia di implementazione, controllo e gestione della sicurezza in modo da agire in accordo alle proprie strategie, individuare le *situazioni d'errore e comportarsi di conseguenza.*

La norma introduce nel campo della sicurezza il concetto di "*Sistema di Gestione*", quale strumento di controllo sistematico e ciclico dei processi legati alla sicurezza, tramite la definizione di ruoli, responsabilità, di procedure formali (sia per l'operatività aziendale che per la gestione delle emergenze) e di canali di comunicazione.
Un Sistema di Gestione della Sicurezza delle Informazioni (ISMS) efficiente, efficace e conforme allo Standard l'ISO/IEC 27002 permette all'organizzazione di:

- implementare politiche e procedure di sicurezza, in accordo con normative cogenti, best practice di riferimento;
- mantenersi aggiornata su nuove minacce e vulnerabilità, e di affrontarle in modo sistematico;
- gestire le aree aziendali a rischio, attraverso la selezione di opportuni controlli di sicurezza;
- creare una cultura della sicurezza all'interno dell'azienda;
- presidiare le attività relative alla generazione di procedure di sicurezza e tracciamento di operazioni critiche;
- trattare incidenti e situazioni critiche, in ottica di prevenzione e di miglioramento continuo del sistema.

La strutturazione secondo lo Standard del Sistema di Gestione della Sicurezza delle Informazioni (ISMS), si sviluppa attraverso l'identificazione degli obiettivi di controllo e l'attuazione dei controlli[27] previsti all'interno delle seguenti aree tematiche (in questo contesto, il termine "controllo" deve essere inteso in senso lato come "strumento di gestione"):

1. Politica della sicurezza dell'informazione (Security policy);

[27] Lo schema del Decreto Legislativo 196/2003 "Codice in materia di protezione dei dati personali" ha preso spunto dallo Standard ISO/IEC 27002, ma mentre lo Standard prende in considerazione tutte le tipologie di informazione, la legge si applica solo ai dati personali.

2. Organizzazione per la sicurezza (Organization of information security);
3. Classificazione e controllo delle risorse (Asset management);
4. Sicurezza del personale (Human resources security security);
5. Sicurezza fisica ed ambientale (Physical and environmental security);
6. Gestione delle operazioni e delle comunicazioni (Communications and operations management);
7. Controllo degli accessi (Access control);
8. Sviluppo e manutenzione del sistema (Information system acquisition, development and maintenance);
9. Gestione degli incidenti (Information security incident management)
10. Gestione della continuità aziendale (Business continuity management);
11. Conformità normativa a leggi, regolamenti, contratti, etc.. (Compliance).

L'**ISO/IEC TR 13335** [28] (*Information Technology – Guidelines of IT Security*) è un Technical Report il cui scopo è quello di fornire delle linee guida per un approccio sistematico alla gestione della sicurezza ICT, che consenta di raggiungere e mantenere il livello di confidenzialità, integrità e disponibilità definito dall'organizzazione all'interno degli obiettivi di sicurezza[29].

Tali indicazioni non riguardano solo gli aspetti di gestione della sicurezza ma anche le misure di dettaglio per l'implementazione e la manutenzione delle procedure. Quindi se gli Standard ISO/IEC 27001 e ISO/IEC 27002 si fermano al "perché" ed al "cosa", il TR 13335 fornisce molti elementi sul "come".

Il TR 13335 era originariamente diviso in cinque parti:

- Parte 1: Concetti e Modelli di IT Security (Concepts and Models for IT security);
- Parte 2: Gestione e Pianificazione della Sicurezza IT (Managing and Planning IT security);
- Parte 3: Tecniche di Gestione della Sicurezza IT (Techniques for the management of IT security);
- Parte 4: Selezione delle contromisure (Selection of Safeguards);
- Parte 5: Guida al management della Sicurezza di Rete (Management Guidance on Network Security).

Nel 2008 la Parte 3 e la Parte 4 sono divenuti ISO e formalizzate al'interno dello Standard **ISO/IEC 27005:2008** (Standard for information security risk and management). La norma, che ricalca i concetti della vecchia ISO Guide 73[30] e ne riusa la terminologia, fornisce delle linee guida sulla gestione del rischio legato alla sicurezza IT e supporta l'applicazione della norma ISO/IEC 27001:2005. Si divide in Valutazione (Assessment) e Trattamento del Rischio, l'Analisi ne è un sottoinsieme. Riporta dettagli precisi per ogni fase e numerosi esempi negli annex informativi.

---

[28] La serie ISO/IEC 13335 che fa parte dei GMITS (Guidelines for the Management of IT Security).

[29] Non trattandosi, dunque, di uno standard non esiste una certificazione ISO TR 13335. Le procedure ISO prevedono, infatti, l'emissione di un Technical Report in alcune circostanze in cui non si possa giungere alla definizione di uno standard vero e proprio o per mancanza di consenso o per la generalità dell'argomento. Il TR 13335 ricade in quest'ultima casistica (Fonte: White Paper "Introduzione agli standard di Sicurezza delle Informazioni ed Informatica" di Alessandro Bottonelli).

[30] ISO Guide 73:2009 (aggiornamento della ISO Guide 73:2002) - "Risk management"; Vocabulary; Guidelines for use in standards.

La norma ISO/IEC 27005 non fornisce tuttavia alcuna specifica metodologia poiché è compito delle singole organizzazione definire un approccio adeguato al contesto di riferimento, in considerazione degli obiettivi di sicurezza che si intendono raggiungere.

6. Modelli di gestione della sicurezza

La Gestione della Sicurezza è un processo ciclico (ISMS – Information Security Management System) il cui scopo fondamentale è, dunque, quello di attuare un ragionevole compromesso tra il costo della sicurezza e i costi della non sicurezza e, raggiungere e mantenere appropriati livelli di confidenzialità, integrità e disponibilità delle risorse del sistema informativo detenute dall'organizzazione nonché di autenticità e di non ripudio delle informazioni trasmesse.
Il modello processuale di gestione della sicurezza (ISMS) trae origine dalle indicazioni fornite:

- dagli attuali Standard internazionali di riferimento:
    - Lo Standard ISO/IEC 27001:2005 "Standard for ISMS";
    - lo Standard ISO/IEC 27002:2007 "Code of Practice for ISMS";
    - lo Standard ISO/IEC 27005:2008 "Standard for Information risk and management".
- dalle Best Practice di riferimento in materia:
    - Linee Guida AIPA "Definizione di un piano per la sicurezza dei sistemi informativi automatizzati nella pubblica amministrazione";
    - NIST (National Institute for Standard and Technology);
    - ISF (International Security Forum);
    - CobiT – Control Objectives of IT Governance (ISACA).

Detto modello si scompone nelle seguenti fasi, ciascuna delle quali prevede lo svolgimento di una serie di attività:

- Fase 1: Definizione delle Politiche di sicurezza aziendali;
    - Individuazione degli Obiettivi di sicurezza aziendali;
    - Strutturazione del modello di gestione della security aziendale (ISMS);
    - Individuazione dei Ruoli e delle Responsabilità;
    - Definizione di Criteri Generali e riferimenti di conformità.
- Fase 2: Analisi dei Rischi:
    - Individuazione e valorizzazione dei beni da proteggere;
    - Individuazione e valutazione degli Impatti, delle Minacce e delle Vulnerabilità cui i beni da proteggere sono esposti (Misura del Rischio);
    - Individuazione delle misure di sicurezza raccomandate e stima dei relativi costi.
- Fase 3: Gestione dei Rischi:
    - Gap Analysis tra le misure di sicurezza raccomandate e quelle già presenti in azienda;
    - Scelta della strategia di gestione del rischio.
- Fase 4: Elaborazione del Piano per la Sicurezza:
    - Pianificazione degli interventi di sviluppo delle misure di sicurezza;

    - Definizione delle specifiche funzionali delle misure di sicurezza;
    - Analisi e studi di fattibilità.
- Fase 5: Definizione di Standard e Procedure di sicurezza:
    - Definizione degli standard e delle procedure specifiche per l'esercizio ed il monitoraggio delle misure di sicurezza.
- Fase 6: Progettazione, sviluppo ed implementazione delle misure di sicurezza:
    - Effettuazione di verifiche architetturali;
    - Realizzazione e collaudo delle misure;
    - Certificazione delle soluzioni;
    - Implementazione delle misure.
- Fase 7: Esercizio delle misure di sicurezza:
    - Gestione delle misure di sicurezza implementate in conformità agli standard ed alle procedure operative definite.
- Fase 8: Monitoraggio:
    - Verifica continua della efficacia delle misure di sicurezza implementate;
    - Reporting;
    - Gestione delle criticità e proposte migliorative.
- Fase 9: Formazione:
    - Progettazione ed erogazione di Piani formativi mirati e differenziati per il personale (crescita del grado di consapevolezza, sensibilizzazione sulle problematiche di sicurezza informatica, sviluppo di specifiche competenze).
- Fase 10: Comunicazione:
    - Definizione ed erogazione di Piani di comunicazione per ciascuna delle fasi del processo di gestione della sicurezza informatica.

Definizione delle politiche di sicurezza

La salvaguardia del patrimonio informativo aziendale è una scelta strategica manageriale volta a consentire e favorire il raggiungimento degli obiettivi di business attraverso:

- la tutela delle risorse informative nel loro valore patrimoniale e reddituale;
- la garanzia della qualità del servizio, venendo incontro alla domanda di fiducia degli interlocutori sociali (stakeholders) interni ed esterni;
- la garanzia della continuità operativa, prevenendo l'interruzione del business anche in condizioni estreme.

Una politica di sicurezza, è una formale dichiarazione degli obiettivi (rientrano negli obiettivi anche la conformità alle normative nazionali, generali e di settore, in materia di sicurezza delle informazioni), delle linee guida strategiche e del modello logico, organizzativo e gestionale definiti per l'attuazione di tale strategia[31].

Tale documento deve, quindi, essere approvato dal Management aziendale, pubblicato e comunicato a tutti i dipendenti

---

[31] Standard ISO/IEC 27002:2005. Paragrafo 5.1 - Information Security Policy. "*Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations*. Management should set a clear policy direction in line with business objectives and demonstrate support for, and commitment to, information security through the issue and maintenance of an information security policy across the organization."

Secondo le indicazioni del Technical Report ISO/IEC TR 13335-2, devono essere previsti tre livelli delle politiche di sicurezza:

- 1° Livello: Politica di sicurezza aziendale ICT (Corporate ICT Security Policy);
- 2° Livello: Politiche di sicurezza dipartimentali ICT (Department ICT Security Policy);
- 3° Livello: Politica di sicurezza specifica di un sistema ICT (System Specific ICT Security Policy).

Dunque, accanto alle Corporate ICT Security Policy, che esprimono gli obiettivi e le strategie per la gestione della sicurezza dei sistemi informativi a livello aziendale, il modello gerarchico adottato dal TR 13335 prevede altresì lo sviluppo:

- delle *Department ICT Security Policy*, politiche di sicurezza che individuano i requisiti funzionali e le regole tecniche e procedurali relativamente a tutte le misure di sicurezza applicabili alle strutture che erogano i servizi di business e/o amministrativi,
- e delle *System Specific ICT Security Policy*, politiche di sicurezza che individuano le regole specifiche di gestione della misura di sicurezza selezionata.

Analisi dei rischi

Presupposto necessario alla scelta della migliore strategia di gestione della sicurezza é la corretta conoscenza dei rischi specifici cui i sistemi informativi aziendali sono esposti.

E' quindi essenziale essere in grado di identificare e valutare i rischi esistenti o potenziali e il loro possibile impatto sull'organizzazione in termini di perdite economiche, violazione normative, rallentamenti dell'operatività, perdita di immagine etc...

L'Analisi dei rischi costituisce uno strumento mirato all'individuazione del quadro generale delle reali esigenze di sicurezza aziendali[32] e si articola nelle seguenti fasi, da compiersi in sequenza ordinata:

- Classificazione degli Asset, ovvero delle informazioni e delle risorse informatiche da proteggere, attraverso la loro valorizzazione. Le informazioni andranno valutate ai fini degli obiettivi di integrità, riservatezza e disponibilità previsti nella definizione delle politiche di alto livello. Le risorse informatiche andranno valutate ai fini degli obiettivi di disponibilità.
- Individuazione e valorizzazione delle minacce e delle vulnerabilità cui gli Asset sono potenzialmente esposti;
- Calcolo del profilo di rischio;
- Identificazione delle protezioni offerte dai controlli identificati dalla ISO/IEC 27001 (contromisure raccomandate);
- Gap Analysis, ovvero valutazione del livello di scostamento tra le contromisure consigliate e quelle esistenti o pianificate all'interno dell'azienda.

Per la scelta della metodologia (qualitativa o quantitativa)[33] o degli strumenti attualmente disponibili sul mercato (ad es. CRAMM, Risk Watch, Expert, etc..) da utilizzare per l'analisi

---

[32] La certificazione ISO/IEC 27001 si basa sui risultati di una formale analisi del rischio.

[33] Le metodologie quantitative si considera preponderante il valore economico delle risorse da proteggere, mentre le metodologie qualitative pongono l'attenzione principalmente sugli aspetti della confidenzialità, integrità e disponibilità dell'informazione. In questo ultimo caso un analisi dei costi-benefici potrà essere eseguita nella successiva fase di gestione del rischio (Risk Management).

dei rischi, è importante ricordare che "… l'analisi del rischio deve identificare minacce a beni, vulnerabilità ed entità del possibile impatto sull'organizzazione, stabilendo il grado di rischio…" (ISO/IEC 27001).
Dunque, il rischio (**R**) si può definire, in via generale, come il prodotto scalare tra la gravità (impatto) delle conseguenze che un evento pericoloso determinerebbe (**I**), e la probabilità che tale evento pericoloso (minaccia) si realizzi (**P**):

$$\mathbf{R} = \mathbf{I} \times \mathbf{P}$$

Tale definizione nel contesto della sicurezza delle informazioni può essere raffinata considerando, per le minacce di tipo deliberato, la probabilità (**P**) come una funzione delle vulnerabilità (**V**) presenti nel sistema e delle motivazioni dell'attaccante, o livello della minaccia (**M**):

$$\mathbf{P} = f\ (\mathbf{V}, \mathbf{M})$$

(per minacce di tipo deliberato)

Per le minacce di tipo accidentale la probabilità (**P**) che un sinistro si verifichi è funzione della vulnerabilità alla minaccia (**V**) e della probabilità intrinseca di accadimento del sinistro (**p**) (ad esempio: probabilità intrinseca di eventi atmosferici, inondazioni, black-out, nella zona considerata)

$$\mathbf{P} = f\ (\mathbf{V}, \mathbf{p})$$

(per minacce di tipo accidentale)

La gravità delle conseguenze (I) è normalmente esprimibile in termini di danno economico subito dall'azienda coinvolta nel sinistro, quindi in valuta corrente o classi di danno individuate da limiti definiti in valuta corrente [34].

Gestione dei rischi

Secondo lo Standard ISO/IEC 27002 le aree di rischio da gestire vanno identificate in base alla politica per la sicurezza e al grado di assicurazione richiesto.
Partendo dall'assunto che la sicurezza totale non esiste, la scelta della strategia di gestione del rischio ha due obiettivi:

- prioritizzare i rischi sulla base delle indicazioni fornite dalle politiche di sicurezza;
- individuare un livello di rischio accettabile per l'azienda (rischio residuo);
- selezionare i controlli maggiormente efficaci e dal costo ragionevole in grado di ridurre i rischi al livello considerato accettabile.

L'identificazione della migliore strategia di gestione del rischio risulta essere, dunque, correlata:

- ai costi sostenibili dall'azienda per ottimizzare il livello di sicurezza esistente;
- ai benefici derivanti dall'approntamento delle misure di sicurezza ottimali;
- all'accettazione di un livello di rischio residuo.

e deve avvenire attraverso:

- la pianificazione in accordo con il Management del piano d'investimento per la gestione dei rischi, quindi l'individuazione dei piani di intervento prioritari;

[34] Fonte: CLUSIT "Linee Guida per l'analisi del rischio" (2002).

- la valutazione dei vincoli di realizzazione dei piani d'intervento (vincoli di tipo temporale, ambientale, economici, etc..).

SELEZIONE DEI CONTROLLI DI SICUREZZA

"… Un sistema di sicurezza può essere paragonato a una catena, composta da vari anelli, ciascuno dei quali influisce in modo determinante sulla sua resistenza. Come in qualsiasi catena, la forza del sistema di sicurezza corrisponde a quella del suo componente più debole…"[35].

Per ridurre o prevenire lo sfruttamento, da parte di una potenziale minaccia, di una vulnerabilità, intrinseca o estrinseca ai beni aziendali, si rende necessaria un'opera di controllo mediante l'applicazione di particolari contromisure protettive rappresentate da azioni, dispositivi, procedure o tecniche.

Con il termine contromisure si indicano, quindi, gli strumenti organizzativi e tecnologici in grado di contrastare e abbattere il livello del rischio, riducendolo ad un livello individuato come accettabile.

Poiché il costo dei controlli di sicurezza deve essere appropriato rispetto al rischio cui deve far fronte un'organizzazione, risulta di fondamentale importanza la scelta del "cocktail" di strumenti più adeguato alle esigenze di business dei diversi servizi dell'organizzazione.

7. Logiche Organizzative per i presidi della sicurezza

L'attuazione dell'ISMS, comporta la definizione di un'infrastruttura organizzativa che si renda responsabile della sicurezza delle informazioni in tutti i suoi aspetti [36] ed assicuri:

- la gestione ed il controllo dei processi e delle attività legate alla sicurezza (ISMS);
- la protezione delle risorse informative aziendali:
    - nei rapporti interni (dipendenti, collaboratori, consulenti, etc..);
    - nei rapporti con le terze parti (clienti, fornitori, partner, etc..);
    - nei casi di affidamento all'esterno delle attività di trattamento (outsourcing).

Di seguito vemgono descritti i principali ruoli e le responsabilità previste dalle normative internazionali e dalla legislazione italiana in materia di gestione della sicurezza.

---

[35] Schneier B. - Sicurezza digitale, Tecniche nuove (Milano 2001)

[36] Standard ISO/IEC 17799. Paragrafo 4.1 – *Organizational Security*. "Objective: To manage information security within the organization. A management framework should be established to initiate and control the implementation of information security within the organization. Suitable management fora with management leadership should be established to approve the information security policy, assign security roles and co-ordinate the implementation of security across the organization. If necessary, a source of specialist information security advice should be established and made available within the organization. Contacts with external security specialists should be developed to keep up with industrial trends, monitor standards and assessment methods and provide suitable liaison points when dealing with security incidents. A multi-disciplinary approach to information security should be encouraged, e.g. involving the co-operation and collaboration of managers, users, administrators, application designers, auditors and security staff, and specialist skills in areas such as insurance and risk management".

IL RUOLO DELLA DIREZIONE

La Direzione, ha la responsabilità di definire gli obiettivi, le linee guida strategiche ed il modello logico-organizzativo di gestione della sicurezza aziendale.

In base alla vigente normativa nazionale in materia di protezione dei dati personali (D.Lgs. 196/2003) tale ruolo coincide con quello del "*Titolare del trattamento dei dati*" cui spettano tutte le "… decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza" (art. 4 lett. f del sopra citato decreto).

Compito della Direzione è, dunque, quello di dar vita ad un'organizzazione di sicurezza, attraverso:

- la strutturazione del modello processuale dell'ISMS;
- l'assegnazione dei ruoli e delle responsabilità nell'ambito della gestione della sicurezza;
- la definizione delle politiche, delle linee guida, delle procedure e delle direttive in materia di protezione delle informazioni;
- la scelta della strategia e degli strumenti per la gestione dei rischi;
- il potere di controllo sullo stato di attuazione dell'ISMS.

IL MANAGEMENT DIVISIONALE E DIPARTIMENTALE

Il Management di livello divisionale e dipartimentale, avendo conoscenza diretta del funzionamento dei propri dipartimenti e delle mansioni del personale, ha la responsabilità di contribuire alla formazione delle politiche di sicurezza, di partecipare ai processi di analisi e di controllo del rischio, all'analisi costi/benefici delle contromisure e al monitoraggio delle attività di sicurezza.

Tale figura può essere ricondotta al ruolo del "Contitolare del trattamento dei dati" cui può essere attribuito, su delega, il potere di controllo e di vigilanza spettante al Titolare del trattamento dei dati (D.Lgs. 196/2003).Il Management di livello divisionale e dipartimentale esercita generalmente il suo ruolo delegando parte dei propri compiti, pur condividendo la responsabilità, al Management operativo, agli specialisti di sicurezza, ai System Administrator ed agli Auditor.

IL MANAGEMENT OPERATIVO

Il Management operativo ha il compito di fornire informazioni operative al personale per pianificare, organizzare e monitorare il sistema di gestione della sicurezza, implementare le politiche, le linee guida, le procedure ed attuare i controlli di sicurezza.

Poiché è generalmente responsabile del processo/servizio con cui viene generato il dato, ed è il proprietario delle applicazioni utilizzate per la sua elaborazione (Proprietario delle Applicazioni/Dati) risulta essere il massimo responsabile della protezione delle informazioni e della sicurezza in generale. A lui verrà imputata ogni negligenza che abbia come conseguenza l'alterazione, la perdita o la divulgazione illecita delle informazioni.

Il suo ruolo coincide con quello del "Responsabile del trattamento dei dati" previsto all'art. 29 del D.Lgs. 196/2003.

L'ADMINISTRATOR

L'Administrator, che a seconda delle risorse amministrate può ricoprire il ruolo di System Administrator o di Network Adminidtrator, ha il compito di sovrintendere alla gestione delle risorse dell'infrastruttura informatica (base dati, applicazioni, sistemi, rete) e di consentirne l'utilizzazione. Generalmente è identificabile con il gestore delle applicazioni/dati, deve essere formalmente individuato ai sensi del Provvedimento del 27 novembre 2008 emanato dall'Autorità Garante per la protezione dei dati in materia di "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" e relativamente agli aspetti di sicurezza è responsabile:

- della gestione e dell'adeguamento dell'infrastruttura informatica a livelli tecnologici tali da garantire la riservatezza, l'integrità e la disponibilità dei dati e dei servizi, dell'implementazione dei meccanismi di sicurezza;
- dell'implementazione e della gestione dei meccanismi di sicurezza secondo le politiche, gli standard e le linee guida che riguardano la sicurezza delle informazioni e la protezione dei dati;
- delle operazioni di back up e, quando si renda necessario, ripristino dei dati (e dei programmi);
- della validazione periodica dell'integrità dei dati e dei supporti (sia on line sia di back up);
- del monitoraggio delle eventuali violazioni al sistema.

GLI UTENTI

Gli utenti sono tutti gli individui che quotidianamente utilizzano, ai fin lavorativi, i programmi ed i dati elaborati dai sistemi aziendali.

La loro responsabilità consiste nell'utilizzare correttamente le applicazioni/dati secondo le prescrizioni dettate dal Management operativo per preservare la disponibilità, l'integrità e la riservatezza delle informazioni., nei limiti dell'autorizzazione e conformemente ai profili/privilegi ad esso assegnati (lettura, scrittura e non cancellazione, modifica, etc.), ottenuta da questo ultimo. Detta figura coincide con quella dell' "Incaricato del trattamento dei dati" definito dal D.Lgs. 196/2003 come la "… persona fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile" (art. 4 lett. h del sopra citato decreto).

8. La Certificazione ISO/IEC 27001

Obiettivo della certificazione ISO/IEC 27001 è quello di attestare che l'organizzazione ha definito un Sistema di gestione della sicurezza delle informazioni (ISMS) conforme a quanto previsto dalla norma.

I benefici diretti conseguenti alla certificazione dell'ISMS risiedono nella:

- formale attestazione da parte di una terza parte fidata (il Certificatore) della conformità dell'organizzazione allo Standard ISO/IEC 27001;
- capacità del sistema di tutelare efficacemente il patrimonio informativo aziendale, attraverso:
    - l'attribuzione di specifici ruoli e responsabilità nell'ambito della gestione della sicurezza;

- la gestione delle aree aziendali a rischio;
- il presidio delle attività relative alla generazione di procedure di sicurezza e tracciamento di operazioni critiche;
- la prevenzione e risoluzione di incidenti.

Indirettamente il conseguimento della certificazione comporta un aumento della fiducia di clienti, fornitori e partner con conseguente accrescimento sul mercato del vantaggio competitivo dell'azienda, ed infine l'attestazione di una situazione di conformità rispetto alle normative nazionali in materia di gestione della sicurezza delle informazioni.

Ai fini della certificazione, dunque, l'organizzazione deve strutturare un ISMS aggiornato, documentato e conforme a quanto previsto dalla norma.

Il modello definito dalla ISO/IEC 27001 per la strutturazione dell'ISMS propone un approccio *PLAN – DO – CHECK – ACT* (modello PDCA[37]) che consente di gestire il miglioramento continuo del sistema e di garantire nel tempo la sua adeguatezza e rispondenza agli obiettivi aziendali.

Nella fase *PLAN*, il modello prevede le seguenti attività:

- Definizione dell'ambito (Scope) di applicazione del sistema di gestione della sicurezza delle informazioni, in termini di caratteristiche dell'azienda, della sua collocazione, beni e tecnologia;
- Definizione delle politiche di sicurezza delle informazioni a livello corporate;
- Definizione di un approccio sistematico per l'analisi dei rischi;
- Identificazione e valutazione dei rischi;
- Definizione della strategia di gestione delle aree di rischio individuate sulla base delle politiche di sicurezza e del grado di assicurazione richiesto (identificazione delle opzioni per il trattamento dei rischi: eliminazione, trasferimento, riduzione);
- Selezione degli appropriati obiettivi di controllo;
- Redazione di una dichiarazione di applicabilità (SOA – Statement of Applicability), che dovrà:
  - documentare gli obiettivi di controllo e i controlli selezionati, nonché esplicitare le motivazioni della loro selezione;
  - registrare e motivare l'esclusione di qualsiasi controllo elencato nell'appendice A della ISO/IEC 27001.

Nella fase *DO* del modello, sono previste:

- Formulazione di un piano operativo di trattamento dei rischi;
- Implementazione del piano;

---

[37] Standard ISO/IEC 27001. Paragrafo 0.2 - *Process Approach*. "…This International Standard adopts the "Plan-Do-Check-Act" (PDCA) model, which is applied to structure all ISMS processes…
*Plan (establish the ISMS)***.** Establish ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization's overall policies and objectives.
Do (implement and operate the ISMS). Implement and operate the ISMS policy, controls, processes and procedures.
*Check (monitor and reviewthe ISMS)***.** Assess and, where applicable, measure process performance against ISMS policy, objectives and practical experience and report the results to management for review.
Act (maintain and improve the ISMS). Take corrective and preventive actions, based on the results of the internal ISMS audit and management review or other relevant information, to achieve continual improvement of the ISMS...."

- Implementazione delle contromisure selezionate;
- Svolgimento di programmi di informazione e formazione;
- Esercizio delle contromisure implementate;
- Adozione di procedure e di altre misure che assicurino la rilevazione e le opportune azioni in caso di incidenti relativi alla sicurezza.

La fase *CHECK*, comporta:

- Esecuzione delle procedure di monitoraggio dell'ISMS;
- Esecuzione di revisioni per l'accertamento del rischio residuo;
- Conduzione di audit interni all'ISMS;
- Esecuzione di review al massimo livello dirigenziale dell'ISMS;
- Registrazione delle azioni e degli eventi che potrebbero avere impatti sulla sicurezza o sulle prestazioni dell'ISMS.

Infine, la fase *ACT* del modello prevede:

- Implementazioni delle azioni migliorative dell'ISMS identificate;
- Implementazione delle azioni correttive e preventive;
- Comunicazione dei risultati;
- Verifica che i miglioramenti raggiungano gli obiettivi identificati alla loro base.

La norma, oltre a descrivere il modello processuale di gestione della sicurezza (PDCA), definisce i controlli da attuare per la protezione delle informazioni. In linea con quanto previsto dallo Standard ISO/IEC 27002 i controlli previsti sono 136 raggruppati nelle 11 sezioni contenute nell'Allegato A alla ISO/IEC 27001 [38] e di seguito riportate.

POLITICA DELLA SICUREZZA DELL'INFORMAZIONE.

E' il primo dei controlli previsti dalla norma[39]. La politica di sicurezza è un documento formale, approvato dal management aziendale, che fornisce le direttive, le linee guida ed il modello logico organizzativo e gestionale definiti dal Management per la sicurezza delle informazioni. Deve essere pubblicata e comunicata, in modo appropriato, a tutti i dipendenti.

La politica di sicurezza deve contenere almeno:

- una breve descrizione degli obiettivi di sicurezza ovvero dei principi e delle normative (aderenza ai requisiti legislativi e contrattuali e Standard) cui il Management intende conformarsi;
- una definizione delle responsabilità per la sicurezza ICT;
- le linee guida di supporto per il raggiungimento degli obiettivi.

Deve essere regolarmente revisionata, ed in caso di cambiamenti particolarmente significativi, la revisione dovrà essere tale da garantirne l'adeguatezza. A tal fine dovrà essere individuato un responsabile per il mantenimento della politica di sicurezza.

---

[38] ISO/IEC 27001 - Annex A "Control objectives and controls".

[39] ISO/IEC 27001 - A.5 "Security policy".

ORGANIZZAZIONE PER LA SICUREZZA. [40]

In seno all'organizzazione deve essere prevista la costituzione di un *Forum* per la gestione della sicurezza. La sicurezza informatica è, infatti, una responsabilità di business che dovrebbe essere condivisa da tutti i membri del Management aziendale.

Per tale ragione, il Forum deve garantire chiarezza nella direzione, supporto visibile nella gestione delle iniziative di sicurezza, ed assicurare che il problema della sicurezza venga affrontato con il giusto impegno ed attraverso un'adeguata allocazione delle risorse.

L'organizzazione deve anche:

- prevedere un coordinamento delle iniziative di sicurezza, attraverso il coinvolgimento all'interno del Forum anche delle funzioni aziendali maggiormente rappresentative di una parte rilevante dell'organizzazione e che dovranno essere coinvolte per l'attuazione dei controlli di sicurezza;
- concordare l'allocazione nell'organizzazione di specifici compiti e relative responsabilità nell'ambito della sicurezza;
- definire l'utilizzo di specifiche metodologie e strutturare il modello processuale di gestione della sicurezza (ISMS);
- servirsi di esperti e specialisti della sicurezza per il coordinamento delle attività all'interno dell'organizzazione e stabilire appropriati contatti con le autorità competenti, e le forze dell'ordine;
- assicurarsi che la sicurezza sia parte della formazione del personale;
- verificare l'adeguatezza e coordinare l'implementazione di specifici controlli di sicurezza per i nuovi sistemi;
- individuare i rischi connessi all'accesso alle risorse informative da parte di terze parti (ad es. consulenti) e definire i controlli da attuare e contrattualmente appropriati requisiti di sicurezza (ad es. accordo di riservatezza);
- definire contrattualmente appropriati requisiti di sicurezza nei rapporti di outsourcing.

GESTIONE DELLE RISORSE. [41]

Obiettivo dei controlli previsti in questa categoria è quello di assicurare un'adeguata protezione ai beni dell'organizzazione. Al riguardo la ISO/IEC 27001 prevede che si proceda:

- all'inventario di tutti i beni (informazioni: database, documentazione,procedure, manuali d'uso, risorse SW - di base, applicativo, di sistema, tool di sviluppo,… - e HW - monitor, modem e strumenti di communication quali router e fax …) , attraverso l'identificazione e la documentazione del responsabile e della classificazione di sicurezza;
- alla classificazione delle informazioni, attraverso:
    - la definizione di linee guida che identifichino i vari livelli dell'informazione (pubblica, riservata, segreta, personale, sensibili etc..)
    - la previsione dei controlli associati alle informazioni critiche aziendali;

[40] ISO/IEC 27001 - A.6 "Organization of information security".

[41] ISO/IEC 27001 - A.7 "Asset management".

- la predisposizione di procedure inerenti l'etichettatura ed il trattamento (copia, archiviazione, trasmissione, distruzione) delle informazioni classificate in accordo con le linee guida.

SICUREZZA DEL PERSONALE. [42]

Obiettivo dei controlli è ridurre il rischio della commissione di errori umani, violazioni, frodi o uso improprio delle strutture dell'organizzazione. A tal fine è necessario che l'azienda:

- includa la sicurezza nella Sicurezza nella definizione delle responsabilità del lavoro attraverso:
  - lo screening del personale. All'atto dell'assunzione dovrebbero essere richiesti o verificati l'identità, le referenze personali, il curriculum vitae, i titoli di studio, etc..
  - la stipula di accordi di riservatezza. I termini e le condizioni di impiego dovrebbero illustrare al riguardo diritti e responsabilità giuridiche.
- proceda ad un adeguata educazione ed addestramento del personale alla sicurezza, attraverso corsi di formazione sulle politiche, le procedure e gli strumenti inerenti la gestione della sicurezza;
- definisca procedure per la segnalazione degli incidenti e dei malfunzionamenti, affinché si possano minimizzare i danni, tenere traccia degli eventi critici e mettere a frutto l'esperienza di avvenimenti precedenti;
- definisca provvedimenti disciplinari in caso di violazione delle leggi in materia di sicurezza.

SICUREZZA FISICA ED AMBIENTALE. [43]

I controlli previsti dalla ISO/IEC 27001 in questa sezione sono diretti ad impedire l'accesso non autorizzato, il danneggiamento e l'interferenza all'interno del flusso delle informazioni, la perdita o il danneggiamento dei beni del sistema e l'interruzione delle attività economiche, la manomissione o il furto delle informazioni.

Al riguardo:

- il perimetro di sicurezza deve essere chiaramente definito:
  - l'accesso fisico alla struttura deve essere controllato tramite un'area di reception e consentito solo al personale autorizzato;
  - tutte le uscite di sicurezza del perimetro devono essere allarmate e tenute chiuse;
- i visitatori delle aree di sicurezza dovrebbero essere supervisionati, l'ora e la date dell'ingresso registrati e i diritti di accesso regolarmente controllati;
- le macchine fotocopiatrici, fax devono essere ubicate all'interno del perimetro di sicurezza;
- gli uffici che ospitano terze parti devono essere fisicamente separati da quelle gestite dall'organizzazione;

---

[42] ISO/IEC 27001 - A.8 "Human resources security".

[43] ISO/IEC 27001 - A.9 "Physical and environmental security".

GESTIONE DELLE OPERAZIONI E DELLE COMUNICAZIONI. [44]

Le procedure operative identificate per la gestione della Sicurezza devono essere documentate e soggette a processo di manutenzione. Esse includono:

- istruzioni in caso di condizioni anomale, chi contattare in caso di necessità, riavvio del sistema e procedure di recovery, procedure di back up e di restore, etc..;
- operazioni di change control: identificazione e registrazione, valutazione degli impatti, procedura di approvazione, etc..;
- procedure operative da adottarsi in caso di incidente;

Gli ambienti di sviluppo devono essere separati da quelli operativi. Le attività di test e di sviluppo, infatti, possono causare seri problemi all'ambiente operativo (ad es. cancellazioni involontaria dei file o system failure). L'ambiente di sviluppo deve essere delicato anche in ragione del fatto che altrimenti esisterebbe la reale possibilità di introdurre codice non autorizzato o non testato. Quindi, compilatori ed editor non dovrebbero essere utilizzati in ambiente operativo e dovrebbero esistere differenti procedure di log on.

Per minimizzare il rischio della presenza di falle nei sistemi alle falle, devono essere definiti chiaramente i criteri per l'accettazione dei sistemi e per la verifica delle loro performance.

Onde assicurare l'integrità dei programmi utilizzati dall'azienda contro i danni derivanti da malicious software è necessario definire regole per l'utilizzo delle licenze (proibizione di software non autorizzato), l'installazione di soluzioni antivirus e procedure di controllo periodico delle macchine finalizzato alla ricerca di software sospetto/non autorizzato.

Onde assicurare l'integrità delle informazioni nella fase della conservazione è necessario regolamentare le attività di backup e restore attraverso la definizione di politiche e procedure che prevedano:

- l'archiviazione dei supporti in luoghi protetti;
- attività di test periodico dei backup;
- il periodo di mantenimento delle copie di back up;

Al fine di salvaguardare le informazioni in fase di trasmissione e proteggere l'infrastruttura di rete:

- le responsabilità operative per la rete dovrebbero essere disgiunte da quelle per i sistemi;
- dovrebbero essere stabilite le responsabilità e le procedure per la gestione degli apparati in remoto;
- dovrebbe essere preservata l'integrità e la confidenzialità dei file che passano sulla rete ad esempio mediante l'utilizzo di sistemi di crittografia.

Per prevenire il danneggiamento dei beni aziendali e l'interruzione dei servizi di business è necessario che l'esportazione delle informazioni, dei media (nastri, disk, cdrom, tc…), e della documentazione ad essi relativa venga autorizzata dell'organizzazione.

Onde evitare il rischio di perdite, modificazioni o scambio di informazioni e software tra organizzazioni devono essere:

- stabilite le responsabilità e le procedure per il controllo e la notifica delle trasmissioni/ricezioni;

[44] ISO/IEC 27001 - A.10 "Communications and operations management".

- indicate le proprietà dei beni o il copyright sul software e sulla documentazione;
- protette le informazioni tramite tecniche crittografiche;
- stabilite procedure di sicurezza per il trasporto delle informazioni (es. trasporto in contenitori chiusi).

CONTROLLO DEGLI ACCESSI. [45]

Obiettivo dei controlli previsti in questa sezione dalla ISO/IEC 27001 è di assicurare la correttezza e la sicurezza delle operazioni connesse al trattamento delle informazioni.

Per quanto attiene la definizione delle regole per l'accesso alle informazioni ed ai sistemi di informazione è sempre opportuno stabilire policy del tipo: "è generalmente proibito se non esplicitamente permesso" piuttosto che "è permesso se non espressamente proibito" e procedere secondo le seguenti direttive:

- i diritti di accesso devono essere congruenti agli scopi lavorativi;
- ad ogni utente dovrebbe essere:
    - fornito un ID univoco, in modo da poter risalire alle relative responsabilità e l'indicazione scritta dei suoi diritti di accesso;
    - richiesto di firmare una dichiarazione di accettazione delle condizioni di accesso;
- deve essere mantenuta una registrazione di tutti gli utenti abilitati e devono essere defnite delle procedure per la verifica periodica del la correttezza delle registrazioni (raccomandato ogni 6 mesi per diritti di accesso utente e 3 mesi per privilegi speciali);
- si deve procede all'immediata revoca dei diritto di accesso nel caso l'utente sia dimissionario o venga licenziato.

In merito alle regole per l'utilizzo della password deve essere richiesto all'utente di firmare una dichiarazione di assunzione di responsabilità in caso di comunicazione della password. Al riguardo tutto il personale dovrebbe essere avvertito di:

- non rivelare la password;
- evitare di tenerla scritta;
- cambiare la password ogni qualvolta si ritenga compromessa;
- selezionare password robuste (min. 8 caratteri, niente nomi, uso caratteri speciali,..);
- cambiare password ad intervalli regolari;
- bloccare il terminale quando non utilizzato.

Al fine di proteggere i servizi di rete, occorre controllare tutti gli accessi provenienti dall'interno e dall'esterno dell'infrastruttura informatica. Al riguardo:

- dovrebbe essere implementata una politica che regolamenti l'utilizzo della rete e dei servizi di rete ed indichi le procedure di autenticazione da implementare;
- tutte le connessioni esterne (es. dial up) dovrebbero prevedere meccanismi di autenticazione;
- tutte le porte diagnostiche dovrebbero essere controllate.

Al fine di prevenire accessi non autorizzati alle macchine, occorre prevedere apposite procedure

[45] ISO/IEC 27001 - A.11 "Access Control".

di log on che:

- segnalino che l'accesso è consentito ai soli utenti autorizzati;
- limitino il numero di log on conclusi con insuccesso (raccomandato tre volte);
- traccino i tentativi falliti;
- stabiliscano un tempo ragionevole prima di poter re-iniziare la procedura di log on;
- visualizzino i tentativi di log on falliti;
- monitorino accessi ed attività (log event).

Relativamente alle attività di controllo dei log event occorre sottolineare che essa risulta di fondamentale importanza per la sicurezza del sistema e dovrebbe essere pianificata ed effettuata ad intervalli regolari.

Tutte le macchine dovrebbero essere temporalmente sincronizzate, al fine di dare attendibilità ai file di log.

SVILUPPO E MANUTENZIONE DEL SISTEMA. [46]

I controlli previsti in questa sezione sono finalizzati ad garantire la sicurezza dei sistemi in termini di sviluppo e manutenzione.

Al riguardo occorre che l'azienda stabilisca i requisiti di sicurezza ed i controlli da effettuare relativamente alle modifiche di sistema od all'acquisizione di nuovi sistemi.

Per quanto attiene i sistemi applicativi, occorre sia controllare i dati di input (out-of-range, caratteri invalidi, dati incompleti o inconsistenti) che verificare la rispondenza a questi ultimi dei dati di output.

Nel caso di aggiornamento dei sistemi operativi, le operazioni di "update" a librerie dovrebbero essere effettuate solo a seguito di debita autorizzazione e debitamente tracciate. Inoltre, il codice dovrebbe essere scaricato nella macchina solo dopo avere dato evidenza dell'opportuno testing della procedura di accettazione.

Ogni volta si scambi il S.O. per installare una nuova release sarebbe bene svolgere tutti i test di "non regressione" al fine di appurare che il software applicativo non sia stato inficiato dalle modifiche.

Infine, le modifiche a pacchetti software pre-confezionati sono altamente sconsigliate, poiché è necessaria l'autorizzazione del fornitore, e la manutenzione del prodotto decade.

GESTIONE DEGLI INCIDENTI.[47]

L'attuazione del controllo consente di assicurare che qualsiasi fatto o debolezza inerente alla sicurezza delle informazioni venga prontamente comunicato all'interno dell'organizzazione in modo che possano essere presi tempestivi provvedimenti.

In tale contesto per incidente s'intende qualsiasi evento che impatta o minaccia di impattare sulla sicurezza delle informazioni, ovvero di uno o più sistemi o dispositivi informatici, intesa come la possibilità di comprometterne le proprietà di confidenzialità, integrità e disponibilità.

Nella realtà organizzativa un incidente di sicurezza è generalmente identificabile come una

---

[46] ISO/IEC 27001 - A.12 "Information system acquisition, development and maintenance".

[47] ISO/IEC 27001 – A.13 "Information security incident management"

violazione delle politiche di sicurezza o la minaccia che tale violazione si stia concretizzando. L'organizzazione deve strutturare un processo di gestione degli incidenti di sicurezza in modo da garantire alla Direzione una visione precisa e puntuale dei rischi e delle perdite, oltre che un valido metodo di prevenzione.
Devono altresì essere definite le procedure per la gestione degli incidenti rilevanti ai fini della sicurezza delle informazioni in conformità alle vigenti normative nazionali. Tali procedure devono descrivere le finalità, le modalità, i criteri di utilizzo ed i tempi di tenuta dei log rilevanti ai fini della ricostruzione degli incidenti.

GESTIONE DELLA CONTINUITÀ AZIENDALE. [48]
Obiettivo del controllo è minimizzare gli effetti legati all'interruzione della continuità operativa attraverso il ripristino dei servizi critici in tempi accettabili.
Al riguardo è necessario strutturare un sistema di gestione attraverso il quale si identifichino i rischi legati all'interruzione dei processi critici in termini di probabilità di accadimento e relativi impatti per l'organizzazione (sia in termini di danni che di tempi di recupero)
Output di questo processo è il Piano di Continuità Operativa o *Business Continuità Plan* (BCP). All'interno del piano vengono operativamente trattati tutti gli eventi atti a compromettere la continuità operativa aziendale, onde garantire un'organizzata ed efficiente gestione delle conseguenze di un evento imprevisto ed assicurare il ripristino dei servizi critici entro i tempi definiti.

Nel piano sono descritti:

- i ruoli e le responsabilità delle figure coinvolte nel piano;
- la classificazione degli eventi dannosi;
- le condizioni per l'attivazione delle singole procedure identificate nel piano;
- le procedure di emergenza da porre in essere per contenere i potenziali impatti al verificarsi di eventi dannosi;
- le procedure operative alternative;
- le procedure di ripristino successive all'evento;
- le liste di reperibilità.

Il piano deve essere oggetto di manutenzione ed aggiornamento periodici, e rivalutazione a fronte di particolari accadimenti (ad es. cambio di strategia aziendale, cambio di sede aziendale, modifiche legislative, etc…).

CONFORMITÀ. [49]
Ultimo punto di controllo previsto dallo Standard ISO/IEC 27001 riguarda la conformità normativa (leggi, regolamenti, contratti, etc..) ed alla politica di sicurezza.
Per quanto attiene la conformità normativa è necessario che l'azienda proceda all'identificazione di tutti i requisiti statutari, legislativi e contrattuali che devono essere esplicitamente definiti e documentati per ciascun sistema informativo. Al riguardo l'ISO/IEC 27001 fa esplicito

[48] ISO/IEC 27001 - A.14 "Business continuity management".

[49] ISO/IEC 27001 - A.15 "Compliance".

riferimento alle normativa in materia di:

- Protezione della proprietà intellettuale (Copyright);
- Protezione dei dati personali (Privacy);
- Protezione dei sistemi informatici;
- Regole in materia di sistemi di crittografia;
- Protezione delle registrazioni aziendali.

9. Conclusioni

La gestione della sicurezza informatica, nonostante le numerose iniziative normative sia a livello nazionale che comunitario, continua ad essere nel nostro paese un tema residuale, poiché all'interno delle organizzazioni non esiste ancora la percezione del valore reale dell'informazione e della sua vulnerabilità.
Gestire la sicurezza informatica in un'organizzazione complessa come può essere una pubblica amministrazione o una azienda privata è certamente un'attività che richiede una particolare attenzione ed un approccio multidisciplinare e consapevole che tenga conto, oltre che della tecnologia, anche del fattore umano e degli aspetti metodologici e di processo.
Capire bene il valore dell'informazione è il primo passo da compiere.
E' necessario altresì cambiare la mentalità dei dipendenti, dei consumatori e dei cittadini, che tendono a considerarsi semplici spettatori invece di attori respondabili, dando priorità all'educazione in materia di sicurezza.
Occorre integrare la sicurezza informatica all'interno delle principali aree amministrative e di business, con un conseguente incremento della visibilità e delle risorse.
Bisogna spingere verso un cambio di prospettiva della compliance che da passiva, imposta dalle normative e dalla legge, deve diventare attiva ovvero prodotta spontaneamente dalle organizzazioni attraverso la definizione di politiche di sicurezza. Al riguardo, i temi della privacy e della protezione dei dati personali devono essere affrontati con un approccio proattivo allo scopo di minimizzare i rischi bel aldilà degli obblighi di legge.
I rischi devono essere individuati e valutati non attraverso un approccio empirico bensì sulla base di metodologie internazionali, in grado di oggettivizzare i risultati rendendoli credibili e confrontrabili.
Le misure di sicurezza devono essere selezionate in base ai risultati di una formale analisi dei rischi seguendo le indicazione fornite dall'ISO/IEC 27001 riconosciuto non solo a livello internazionale come standard di certificazione, ma anche dalle normative comunitarie e nazionali come lo standard di riferimento per la gestione della sicurezza informatica.

Rivista elettronica di Diritto, Economia, Management

N. 1 - 2010 · pp. 278-285

e-Learning
Metodologie e Tecnica

Edoardo Limone

Abstract: Negli ultimi anni l'applicazione di tecnologie di formazione a distanza si è ampliata sia nel numero di risorse impiegate che nella tipologia di pubblico di riferimento. L'Europa ha cercato di delineare una strada comune per lo sviluppo di queste tecnologie ma spesso, chi le adotta, si trova davanti a molteplici prodotti e standard. Nasce così una falsa credenza ossia che la tecnologia abbia a prevalere rispetto il metodo con cui la formazione viene erogata. Scopo dell'articolo è invertire tale punto di vista, concentrando l'attenzione prima sul percorso formativo e poi sulle modalità di erogazione. L'e-learning diviene così una tecnologia basata sulla sinergia lavorativa di più figure professionali (docenti, tecnici, discenti, etc...) ma anche un valido supporto per la crescita di aziende, dipendenti e giovani, unico per le sue peculiarità e potenzialità nella fase di apprendimento.

In recent years the application of technologies for distance learning has expanded in the number of resources used and in the type of audience. Europe has tried to outline a common way for the development of these technologies, but often, who adopt them, are faced with multiple products and standards. The result is a false belief that the technology has to take precedence over the method by which training is delivered. The purpose of this article is to reverse this point of view, focusing first on training and then on the method of payment. The e-learning becomes a technology based on the synergy of working as professionals (teachers, technicians, students, etc ...) but also a valuable support for growing businesses, employees and young people, unique in its characteristics and potential in the learning phase.

Parole chiave: e-Learning, formazione a distanza, SCORM, ADL, Europa, Piano di Lisbona, piattaforma, NATO

Sommario: 1.Introduzione al problema - 2.Il panorama delle piattaforme e-Learning - 3.Problemi di metodo e standard - 4.Organizzazione di un corso e-Learning - 5.Il contesto internazionale: Europa e Mondo - 6.Conclusioni e casi di eccellenza

Articolo pervenuto il 5 ottobre 2010, approvato il 22 novembre 2010

1. Introduzione al problema

Si sente spesso parlare di e-learning. Negli ultimi anni sono proliferate le università telematiche, le aziende hanno creato portali e-learning per formare i propri dipendenti, le scuole hanno aggiunto servizi di formazione a distanza per estendere i servizi ma, nonostante se ne senta molto parlare, pochi hanno davvero chiaro cosa sia e quali siano i problemi ad esso connessi. Per rispondere alla prima domanda facciamo affidamento al CNIPA che definisce e-learning la: "metodologia didattica che offre la possibilità di erogare contenuti formativi elettronicamente (e-learning), attraverso reti Internet o reti Intranet. Per l'utente rappresenta una soluzione di apprendimento flessibile, in quanto facilmente personalizzabile e facilmente accessibile"[1].
Anche se apparentemente tecnica, questa definizione raccoglie al proprio interno una moltitudine di quesiti e aspetti di natura metodologica, non ultima la riflessione su come un corso formativo debba essere impostato. Occorre quindi scindere il problema di natura tecnica dal problema di natura metodologico-organizzativo dando, come spesso accade, maggior risalto a quest'ultimo piuttosto che ai risvolti tecnici. L'ampia diffusione di Internet ha reso infatti possibile a ciascun utente la creazione della propria piattaforma e-learning. Tale creazione avviene in modo economico (spesso gratuito) e senza enormi sforzi ma, una volta creata la struttura tecnologica rimarrebbe il problema più serio: con quali dati popolarla.
I docenti fanno spesso uso di una terminologia chiave: "*percorso formativo*". Tale percorso viene studiato il più possibile in base alle esigenze dello studente solo che, in una classe universitaria di oltre 180 discenti è difficile operare percorsi granulari mentre con l'e-learning diviene più semplice. Già questa prospettiva complica molto il percorso di creazione dei contenuti formativi ma d'altro canto creare percorsi formativi "standard" farebbe perdere uno dei valori aggiunti dell'e-learning: il controllo capillare dell'andamento di ogni singolo studente. Questa premessa era dunque doverosa per far comprendere al lettore la differenza fondamentale tra gli aspetti tecnici e quelli metodologici e di organizzazione.

2. Il panorama delle piattaforme e-Learning

Operando una prima analisi tecnica potremmo già fare una prima distinzione: esistono piattaforme gratuite e piattaforme a pagamento. La fondamentale differenza tra le due è legata ai servizi, alla modalità di sviluppo e alle esigenze che si vogliono raggiungere. Una piattaforma a pagamento è, normalmente, compatibile ad un numero più elevato di standard di interoperabilità e dovrebbe garantire una stabilità maggiore seguita da aggiornamenti costanti. Spesso però ci si orienta verso piattaforme gratuitamente prelevabili dalla rete, per poi personalizzarne l'aspetto e le funzionalità. Le piattaforme a pagamento, tendono a garantire anche servizi di assistenza molto più vicini alle esigenze cliente. Le piattaforme attualmente sulla rete consentono di creare contenuti più o meno multimediali anche se non direttamente

[1] Vademecum CNIPA "VADEMECUM PER PROGETTI FORMATIVI IN MODALITÀ E-LEARNING" - Quaderno n.32 " - Pag. 7

SCORM compatibili. Alcune realtà tecnologiche permettono anche la videochat tra il docente e il discente, l'acquisto dei corsi e la gestione degli aspetti formativi e amministrativi dello studente in un'unica soluzione. Applicativi web di questo tipo vengono ceduti gratuitamente ad utenti privati e pubblici, fornendo potenti strumenti che però rischiano di diventare inutili con un utilizzo non corretto. Alcune tra le piattaforme più rinomate nell'ambito Open Source sono:

- Moodle[2].
- Saba[3].
- Ilias[4].

Tra queste spicca, per notevole diffusione e notorietà Moodle anche se Ilias risulta avere una maggiore apertura verso gli standard. Ilias è, di fatti, la piattaforma e-learning usata in ambito NATO. Come dicevamo le piattaforme non creano contenuti SCORM, li leggono solamente, né interpretano i contenuti e creano i percorsi formativi secondo quanto è definito all'interno del pacchetto SCORM. Creare gli SCORM richiede strumenti di produzione che esistono sia in forma gratuita (ad es. EXE Learning), sia in licenza commerciale (ad es. Lectora). Quando si tenta di creare un corso e-Learning, ci si trova comunque davanti ad una varietà non indifferente di problematiche e quasi nessuna è di natura tecnica. Principalmente si parla di problemi legati al metodo di formazione e al percorso disciplinare da definire per lo studente. Per questo motivo, nei prossimi capitoli, verranno affrontate tematiche non direttamente collegate agli aspetti tecnici, bensì ad aspetti di organizzazione e formazione.

3. Problemi di metodo e di standard

Cominciamo a fare un po' di chiarezza sul panorama e-learning con un'affermazione apparentemente scontata: l'aspetto più importante nella formazione a distanza è il contenuto formativo ed il modo in cui esso viene trasmesso al discente. Occorre quindi avere una metodologia di insegnamento ad hoc, supportata da un comparto tecnico opportunamente studiato per i corsi che si decide di erogare. Questa affermazione apre molteplici congetture, non ultima una sugli standard. Nel mondo e-learning esistono diversi standard, uno di questi è lo SCORM. Prenderemo in esame proprio questo standard per comprendere due affermazioni, la prima è che uno standard potrebbe essere non necessario all'ente erogatore dei corsi. La seconda è che tanto si parla di standard quanto bisogna stare attenti al significato stesso di questa parola. Lo SCORM per la precisione non è uno standard internazionalmente riconosciuto: infatti non esistono standard *de iure* ma solo standard *de facto*. Lo SCORM è divenuto standard *de facto* perché garantisce specifiche affidabili di: riutilizzo dei corsi, tracciamento dei risultati, catalogazione degli oggetti didattici (di seguito chiamati SCO- Sharable Content Object), e una notevole flessibilità nella modalità di esecuzione del corso (in sequenza o con percorsi

[2] http://moodle.org

[3] www.saba.com/

[4] www.ilias.de

alternativi). Tuttavia, il fatto che esso non sia uno standard *de iure* e che non ne esista uno, è indicativo della impossibilità di definirne uno valido a livello globale. Prima di affrontare questo tema è opportuno osservare anche il lato tecnico della faccenda. Lo SCORM altro non è che un file che contiene al suo interno le risorse didattiche (la cui unità minima viene chiamata asset) e la "logica" con cui vengono presentate allo studente. Ovviamente entrambi i componenti dovranno essere leggibili ed interpretabili dalle piattaforme e-learning che, pertanto, dovranno rispondere a rigidi standard di compatibilità. Immaginando che la piattaforma sia "SCORM compatibile", gli erogatori dei corsi dovranno produrre file SCORM validi e, per farlo, dovranno aver ottenuto una certificazione dall'ente che ha creato le linee guida per la creazione di contenuti SCORM: l'ADL[5] (Advanced Distribuited Learning). Ecco quindi che la "trafila" da percorrere per avere contenuti standard, ma sempre de facto, è lunga e comporta un dispendio di tempi e costi. Una volta ottenuta la certificazione ed effettuati i controlli sui corsi prodotti, si può garantire l'interoperabilità all'estero, ammettendo che il destinatario dei corsi abbia scelto lo SCORM come standard e non un altro. La prima domanda a cui bisognerebbe porsi è se effettivamente debba essere necessario ricorrere ad uno "standard" piuttosto che produrre contenuti formativi *ad hoc*.

Se si volesse vendere i propri contenuti all'estero potrebbe apparire evidente che lo standard, anche se de facto, sia la soluzione più comoda. Tuttavia c'è chi ritiene che un modello di lezione unico e studiato appositamente per lo studente, anche se non annoverabile tra gli standard, possa avere un valore aggiunto e che uno standard de facto, proprio perché de facto, rischia di diventare più un limite che un aiuto. Proprio questa diversità di vedute impedisce la formazione di uno standard *de iure*. Dove è scritto ad esempio che un corso debba essere venduto o comunque ceduto? È infatti possibile accogliere gli studenti stranieri nella propria piattaforma, senza alcun tipo di problema legato a compatibilità e/o comunicazioni tra le piattaforme (argomento che per complessità tecnica richiederebbe un documento a sé). Il corso verrebbe presentato nella lingua necessaria alla comprensione degli studenti e l'accesso verrebbe reso fattibile attraverso la comunicazione tra le due università e dalle infinite risorse tecnologiche di cui si può far uso. Un altro esempio di scostamento dallo SCORM potrebbe essere ipotizzabile in corsi che richiedono test e valutazioni particolari e che non sono comprese nella modalità SCORM. Lo SCORM, la cui versione più diffusa è la 1.2, sta cercando di distribuire la versione 2004 che introduce notevoli miglioramenti ma che tutt'ora risulta di difficile integrazione in moltissime piattaforme. Pertanto viene poco considerato come standard.

Guardando il panorama tecnologico da un altro punto di vista, si potrebbe affermare che vi siano molteplici possibilità di scelta da adottare. Il fornitore dei corsi potrà affidarsi tanto allo SCORM quanto ad una tecnologia ad hoc, tuttavia l'aspetto critico della creazione di contenuti e-learning rimane la metodologia e l'organizzazione. Erogare contenuti e-learning, significa garantire allo studente una continuità di servizi e di assistenza che, per un docente non esperto, può trasformarsi in una realtà di difficile gestione. Un altro problema è

[5] ADL si è creata nel 1997 per standardizzare e ammodernare la diffusione delle tecniche formative. A supervisione del lavoro svolto da ADL c'è direttamente il Dipartimento della Difesa americano e più precisamente la "Secretary of Defense for Personnel and Readiness (OUSD P&R)" maggiori informazioni a http://www.adlnet.gov

l'aggiornamento dei contenuti. L'e-learning obbliga il docente prima e la struttura poi ad un costante aggiornamento dei percorsi formativi che, proprio per la loro costante presenza in rete, non possono rischiare di diventare obsoleti. Questa procedura di "manutenzione" del corso, vede impegnate più figure professionali: dai tecnici fino all'istituzione che eroga il corso.

4. Organizzazione di un corso e-Learning

Il requisito minimo che una struttura e-learning dovrebbe avere, per poter erogare corsi di qualsiasi tipo, dovrebbe contenere:

1) Lo staff tecnico, responsabile dell'effettiva fruibilità del corso sulla piattaforma e quindi sulla rete ma anche della creazione dei contenuti formativi dal punto di vista meramente tecnico.
2) Lo staff docente, responsabile della creazione dei contenuti sotto il profilo dei percorsi formativi.
3) Lo staff amministrativo, responsabile dei rapporti con gli studenti ed i docenti, nonché principale attore nel panorama di sviluppo dei contenuti formativi.

Questi tre nuclei lavoreranno a stretto contatto ogni qualvolta si decida di "mandare online" tanto un intero corso formativo, quanto una singola dispensa. Chiaramente lo staff tecnico deve supportare quello dei docenti: offrendo soluzioni che permettano la divulgazione del metodo migliore di formazione senza limiti di natura tecnologica, anche se questo comporta la non osservanza degli "standard" di cui abbiamo parlato precedentemente.
Entrando maggiormente nel dettaglio dei contenuti formativi e del percorso formativo possiamo certamente affermare che un punto di attenzione è data dalla suddivisione dei moduli. La possibilità di riusare un corso e-learning dipende molto dall'ampiezza dei vari moduli che compongono un corso. Questo problema è presente sia che usiate o no uno "standard" come lo SCORM. Il problema non è tecnologico ma metodologico. Moduli capillari sono più difficilmente catalogabili ma più facilmente riusabili e, in caso di aggiornamento del corso, rappresentano una strada di economia poiché potrebbero essere parti da non dover aggiornare e quindi meno lavoro da affidare allo staff docenti e tecnico.

5. Il contesto internazionale: Europa e Mondo

Fino ad ora abbiamo esaminato gli aspetti tecnici e metodologici in un'ottica di alto livello ma è altrettanto interessante cercare di fare il punto della situazione inserendo l'e-learning all'interno del quadro europeo: come si è evoluta questa tecnologia e quali sono i principali risultati ottenuti? Come molti lettori sapranno nel 2000 è stato ideato il Piano di Lisbona. Si tratta di una riunione del Consiglio europeo per monitorare lo sviluppo ICT dei Paesi membri e tracciare linee guida che controllino lo sviluppo delle tecnologie.
Già nel 2001 l'Europa, attraverso la Banca Europea per gli Investimenti (di seguito BEI), rilancia l'iniziativa "Innovazione 2000" su cui aveva stanziato crediti tra i 12 e i 15 miliardi di

euro per:

- "infrastrutture ed attrezzature scolastiche: collegamento delle scuole alle reti digitali, attrezzature informatiche, aule per lo studio dell'informatica, biblioteche e università virtuali"[6];
- "strutture per la formazione e programmi volti ad incoraggiare l'uso, da parte degli insegnanti, delle tecnologie dell'informazione e della comunicazione nell'attività didattica"[7];
- "sviluppo di software e di contenuti multimediali a fini didattici e interconnessione tra università e centri di ricerca in tutta l'Unione europea"[8];
- "creazione di parchi scientifici e di incubatrici per promuovere le innovazioni e aprire la strada alla loro applicazione nel mondo del lavoro."[9]

Gli obiettivi dell'iniziativa sono di alto livello ma già in precedenza, nel documento "e-Learning - Pensare all'istruzione di domani"[10] del 25/05/2000, l'Unione Europea afferma:

- "L'iniziativa eLearning si dedicherà a chiarire i modelli didattici innovativi: le nuove tecnologie consentono in particolare di creare nuovi tipi di rapporti tra alunni e insegnanti"

È evidente che la posizione nei confronti di modelli alternativi allo SCORM è ben accetta e che l'Europa, già nel 2000, considerava l'aspetto metodologico e formativo, come cardine della sfida su cui basare l'e-Learning. Dieci anni dopo l'Europa non ha cambiato punto di vista, anzi si può affermare che abbia rincarato la dose. Il 08/09/2010 è stata rilasciata un'importante relazione "*Education at a Glance*" che copre con i suoi obiettivi ben 35 paesi, di cui 25 dell'UE. La relazione conferma che c'è un'effettiva crescita della richiesta di corsi universitari e che le iniziative formative avranno quindi maggiori finanziamenti. Tra queste iniziative c'è chiaramente un riferimento all'e-Learning di cui, però, non si parla direttamente (non essendo oggetto di analisi diretta).Tuttavia sia i dati Europei sia quelli dell'Osservatorio Tecnologico per la Scuola del Ministero della Pubblica Istruzione, non possono essere considerati del tutto aggiornati. L'Osservatorio (http://www.osservatoriotecnologico.it) ha subito l'ultimo aggiornamento il 16 dicembre 2004. La sezione del sito dell'Unione Europea riservata all'e-Learning (http://ec.europa.eu/education/programmes/elearning/index_it.html) non viene invece aggiornata dal 24 maggio 2006.

Sotto molti aspetti l'e-Learning ha trovato una realizzazione fervida all'interno del mondo privato: le aziende hanno compreso l'importanza di trasmettere la conoscenza attraverso gli strumenti che già erano in loro possesso. I siti aziendali hanno aperto una sezione all'e-Learning in cui il dipendente, durante il tempo libero, può seguire corsi di aggiornamento per aspirare ad un miglioramento della propria posizione lavorativa.

Organizzazioni internazionali come la Federazione Internazionale di Croce Rossa e Mezzaluna

---

6 "Piano d'azione eLearning" - ALLEGATO: guida ai programmi e agli strumenti collegati. {COM(2001)172 final,28.3.2001} - Pg. 21 e seguenti.

7 Ibidem

8 Ibidem

9 Ibidem

10 COM(2000) 318 definitivo - Bruxelles 25/05/2000.

Rossa hanno impiegato l'e-learning per fare micro corsi di formazione (30 minuti massimo) per aggiornare i volontari sui metodi di trattamento del virus influenzale. In quella circostanza la Robert Kaufman (capo "dell'influenza team") affermò: "Questi strumenti per aumentare la conoscenza includono consigli di base per le nostre Società Nazionali di Croce Rossa e Mezzaluna Rossa e quindi possono preparare le loro organizzazioni alla pandemia, proteggere il loro personale e i loro volontari, e aiutare a tenere le loro comunità al sicuro".
Parliamo di oltre 180 Società Nazionali che forniscono strumenti e conoscenza tecnica. In casi come questo, in cui il dimensionamento aziendale è veramente elevato, è necessario concentrarsi più che mai sul metodo di creazione dei corsi. Non si può creare contenuto formativo troppo lungo o con contenuti troppo disparato. Bisogna, generalmente, creare corsi mirati, chiari e validi per tutte le filiali. La tecnologia impiegati è un problema realmente marginale: si può scegliere o meno di rispettare gli standard, l'importante è che i contenuti raggiungano tutti gli utenti ovunque essi si trovino. Nel caso della Croce Rossa è facile pensare che il corso preparato avesse l'obbligo di essere eseguito anche su "macchine datate" e che, quasi certamente, avrebbero avuto difficoltà ad appoggiarsi a standard come lo SCORM.

Conclusioni e casi di eccellenza

Abbiamo citato nel corso di questo articolo la NATO, abbiamo discusso delle reali criticità riguardanti l'e-learning, problematiche che hanno origine nei metodi formativi e nelle modalità di erogazione dei corsi prima ancora che nelle tecnologie impiegate. A questo punto è opportuno presentare un caso di eccellenza in ambito militare: un sistema di interscambio corsi tra paesi diversi, bastato su standard SCORM, che unisce un ottimo impiego di tecnologie, un'ottima organizzazione ed un alto riuso dei contenuti formativi.
L'obiettivo che molte aziende internazionali vorrebbero raggiungere è quello di creare contenuti che, nascendo in un paese, siano validi e facilmente comprensibili in altri in cui magari è presente una filiale, un distaccamento o un'azienda partner. Inoltre sarebbe auspicabile che tali contenuti, garantissero un livello di interoperabilità predefinito basato sul modello SCORM. I casi di eccellenza nel riuso dei contenuti hanno sviluppato una metodologia ben precisa: al momento della creazione dei contenuti formativi, uno staff tecnico affianca quello formativo nella creazione dei moduli. Il docente stabilisce quanto debbano essere granulari gli argomenti da affrontare e determina, con l'ausilio del tecnico, come suddividere il corso. Viene quindi creato un percorso formativo i cui contenuti vengono realizzati con l'idea di poterne garantire la traduzione da parte di aziende internazionali, che intendono acquistare tale risorsa. Ad esempio, le tracce video usate all'interno del corso, avranno l'accortezza di contenere la possibilità di sostituire la traccia audio in modo da favorirne la localizzazione. Quando il corso viene venduto/ceduto, l'azienda ricevente acquista la possibilità di impiegare quella risorsa al meglio delle sue potenzialità, aumentando il riuso (inserendola in altri corsi) e favorendone la comprensione mediante la traduzione. L'azienda ricevente dovrà quindi preoccuparsi di fornire un nucleo di traduttori che provvedano alla localizzazione della risorsa. Stiamo parlando di una metodologia che viene creata per far passare lo stesso contenuto in più paesi, riducendo i costi di conversione e massimizzando il riuso. Tuttavia non è detto che

tale modello possa adattarsi a corsi in cui il riuso è scarsamente rilevante, a favore di contenuti molto più mutevoli nel tempo.

La sinergia necessaria tra i vari staff che compongono il panorama dell'e-Learning nasce proprio da questo presupposto: realizzare una metodologia formativa che non abbia la presunzione di imporsi come standard ma che risponda in pieno alle esigenze dello studente, dei contenuti che compongo il corso e degli aspetti tecnologici a disposizione della struttura formativa.