

RIVISTA ELETTRONICA DI DIRITTO, ECONOMIA, MANAGEMENT

Numero 1 - 2014 • Edizione multimediale

Atti del Convegno ANDIG - Roma, 29 ottobre 2013

a cura di Donato A. Limone

FONDATA E DIRETTA DA
DONATO A. LIMONE

Direttore responsabile

Donato A. Limone

Comitato scientifico

Stefano Adamo (Preside di Economia, Università del Salento), Piero Bergamini (Autostrade), Francesco Capriglione (Ordinario di Diritto degli intermediari e dei mercati finanziari, LUISS, Roma), Michele Carducci (Ordinario di Diritto Pubblico, Università del Salento), Ernesto Chiacchierini (Ordinario di tecnologia dei cicli produttivi, Università La Sapienza), Claudio Clemente (Banca d'Italia), Ezio Ercole (Vice Presidente dell'Ordine dei Giornalisti del Piemonte e consigliere della Federazione Nazionale della Stampa Italiana - FNSI), Donato A. Limone (Ordinario di informatica giuridica, Università telematica Unitelma-Sapienza, Roma), Vincenzo Mastronardi (Ordinario Psicopatologia forense, Università La Sapienza, Roma), Nicola Picardi (Professore emerito della Sapienza; docente di diritto processuale civile, LUISS, Roma), Francesco Riccobono (Ordinario di Teoria generale del diritto, Università Federico II, Napoli), Sergio Sciarelli (Ordinario di Economia Aziendale, Università di Napoli, Federico II), Marco Sepe (Ordinario di diritto dell'economia, Università telematica Unitelma-Sapienza, Roma)

Comitato di redazione

Leonardo Bugiolacchi, Antonino Buscemi, Luca Caputo, Mario Carta, Claudia Ciampi, Ersilia Crobe, Wanda D'Avanzo, Sandro Di Minco, Paola Di Salvatore, Pasquale Luigi Di Viggiano, Paolo Galdieri, Edoardo Limone, Emanuele Limone, Giulio Maggiore, Marco Mancarella, Antonio Marrone, Alberto Naticchioni, Gianpasquale Preite, Fabio Saponaro, Angela Viola

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 V, n. 1/2014

ISSN 2039-4926

Autorizzazione del Tribunale civile di Roma N. 329/2010 del 5 agosto 2010

Editor ClioEdu

Roma - Lecce

Tutti i diritti riservati.

È consentita la riproduzione a fini didattici e non commerciali, a condizione che venga citata la fonte.

La rivista è fruibile dal sito www.clioedu.it gratuitamente.

INDICE

Editoriale

Donato A. Limone, Direttore della RivistaPag. 4

L'Istituto di Teoria dell'Interpretazione e di Informatica Giuridica dell'Università
"La Sapienza". Presentazione di Tommaso Edoardo Frosini

Vittorio Frosini.....13

L'Associazione Nazionale dei Docenti di Informatica Giuridica e di Diritto
dell'Informatica (ANDIG). Diario breve (1988-2013)

Donato A. Limone.....22

I nuovi scenari della società dell'informazione: aspetti politici, giuridici, amministrativi e tecnici. Prima Sessione. Coordina i lavori il prof. Francesco Riccobono

Apertura dei lavori

Francesco Avallone, Donato A. Limone, Francesco Riccobono.....29

La convenzione sul *cybercrime* come base del sistema regolatorio universale
per il cyberspazio

Giuseppe Corasaniti30

Legislazione penale e tecnologie dell'informazione: un difficile rapporto tra contenitore
e contenuto

Paolo Galdieri41

Firme grafometriche e tutela dei dati personali

Gianluigi Ciacci50

Punti fermi e criticità nella disciplina del commercio elettronico a dieci anni
dal recepimento della direttiva UE 31/2000

Leonardo Bugiolacchi.....63

Open data e data protection nel cloud computing

Alberto Maria Gambino77

Cloud computing e trattamento dei dati sanitari

Massimo Farina78

La Giustizia telematica <i>Irene Sigismondi</i>	79
<i>Net Neutrality</i> . La neutralità della rete: problemi attuali e prospettive <i>Angela Viola</i>	80
La democrazia elettronica: aspetti teorici e metodologici <i>Wanda D'Avanzo</i>	97
Il voto elettronico: dall'esperienza del progetto "Salento evoting" al prossimo regolamento di voto per gli italiani residenti all'estero <i>Marco Mancarella</i>	102
La protezione dei dati personali nell'evoluzione normativa e giurisprudenziale, europea e nazionale. Il diritto all'oblio <i>Sandro Di Minco</i>	123
Dal diritto di accesso all' <i>open government data</i> : un nuovo paradigma di gestione del patrimonio informativo pubblico <i>Monica Palmirani</i>	124
I nuovi scenari della società dell'informazione: aspetti politici, giuridici, amministrativi e tecnici. Conclusioni prima parte <i>Donato A. Limone</i>	125
Seconda Sessione. Coordina i lavori il Prof. Giovanni Sartor	
Informatica e Diritto tra antinomie e analogie <i>Giancarlo Taddei Elmi</i>	126
Lo Stato e le sue burocrazie digitali <i>Pasquale Luigi Di Viggiano</i>	136
Conservare il documento informatico: una chimera per PA, Imprese e Professionisti? <i>Andrea Lisi</i>	150
Responsabilità dei fornitori di servizi di <i>video hosting</i> : esperienze europee a confronto <i>Marilù Capparelli</i>	158
<i>E-Procurement</i> ed innovazione. Più organizzazione che tecnologia <i>Michele Melchionda</i>	159

Risorse umane digitali: evoluzione informatica e capacità del personale pubblico <i>Giampaolo Teodori</i>	160
Il valore economico del dato pubblico nelle <i>Smart Cities</i> : gli <i>Open Data</i> per lo sviluppo del territorio <i>Luca Caputo</i>	161
Il nuovo programma <i>Horizon 2020</i> <i>Antonio Maria D'Amico</i>	171
<i>Big Data</i> e diritto <i>Sebastiano Faro</i>	172
L' <i>Open Access</i> nella più recente normativa statale: un passo avanti e due indietro <i>Marina Pietrangelo</i>	173
L'evoluzione del modello di amministrazione digitale: dall' <i>e-government</i> all' <i>open government</i> <i>Fernanda Faini</i>	184
I nuovi scenari della società dell'informazione: aspetti politici, giuridici, amministrativi e tecnici. Dibattito e chiusura del Convegno <i>Donato A. Limone</i>	211

Editoriale

In questo numero pubblichiamo gli Atti del Convegno della *Associazione Nazionale dei Docenti di Informatica giuridica e diritto dell'informatica* (ANDIG – www.andig.it) tenuto a Roma il 29 ottobre 2013 presso l'Università telematica Unitelma SAPIENZA e con il patrocinio della stessa università, della SIIG (*Società Italiana di Informatica Giuridica*), di ANORC (*Associazione Nazionale Operatori e Responsabili della Conservazione digitale*), del *Laboratorio di eGovernment (LEG)* della università del Salento. In questo numero sono pubblicate le registrazioni audio-video dei diversi interventi del convegno ed alcune relazioni scritte. Si tratta del primo numero multimediale della Rivista.

Il Direttore della Rivista
Donato A. Limone

Istruzioni per la lettura

Gli interventi dei relatori del Convegno ANDIG tenutosi a Roma il 29 ottobre 2013 presso l'Università telematica Unitelma SAPIENZA sono riportati in versione integrale sotto forma di MediaBook a cui è possibile accedere cliccando semplicemente sull'immagine di anteprima raffigurante l'autore. Al click si aprirà il MediaBook in una nuova finestra del browser Internet del dispositivo.

Nel caso si disponga della versione cartacea della rivista, per accedere al MediaBook è sufficiente leggere l'apposito *qr-code* mediante uno smartphone o un tablet.



Con il prodotto editoriale **MediaBook**, CLIOedu ha sviluppato un sistema di trasmissione del sapere multicanale ed interattivo: l'efficacia dei contenuti didattici e dell'esperienza formativa nella sua totalità è accresciuta dalla positiva sinergia tra la versatilità dell'ipertesto e la ricchezza del prodotto audiovisivo.

Le espansioni multimediali dei **MediaBook CLIOedu** si integrano perfettamente con le attività tradizionalmente legate alla lettura, come la possibilità di aggiungere annotazioni, saltare da un capitolo all'altro dell'indice e inserire segnalibri nei punti di maggiore interesse.

Autori di questo numero

Leonardo Bugiolacchi

Dottore di ricerca in Informatica giuridica e diritto dell'informatica nell'Università "La Sapienza" di Roma, è stato per molti anni docente di "Diritto commerciale" e di "Diritto delle società" nell'Università Unitelma Sapienza di Roma, ove attualmente dirige il Master di I livello in "Infermieristica forense". Ha insegnato ed insegna in numerosi master universitari dedicati al commercio elettronico ed in generale al diritto delle tecnologie dell'informazione e della comunicazione. Avvocato civilista in Roma, si occupa prevalentemente di diritto della responsabilità civile e di diritto delle nuove tecnologie, con particolare riferimento alla disciplina del commercio elettronico, agli illeciti commessi on line ed alla responsabilità degli internet service providers, al diritto d'autore in rete. E' autore di numerosi saggi ed articoli in materia di responsabilità civile e di diritto delle tecnologie dell'informazione e della comunicazione, pubblicati sulle più importanti riviste giuridiche.

E-mail: avvleonardobugiolacchi@gmail.com

Luca Caputo

Professore a contratto di "Sociologia dell'Ambiente e del territorio" presso l'Università del Salento e svolge attività di docenza in materia di Marketing territoriale, Comunicazione pubblica e Turismo digitale nel Master in Management Pubblico e eGovernment - Università del Salento. Nella stessa Università è componente del Laboratorio di eGovernment, all'interno del quale si occupa dello studio e della ricerca in tema di ICT applicate allo sviluppo urbano, turistico e territoriale. Già professore a contratto nell'Università telematica Telma-La Sapienza di Roma dell'insegnamento di "Sociologia della comunicazione elettronica", è consulente per gli Enti Locali in tema di Pubblica Amministrazione Digitale.

E-mail: ellecaputo@gmail.com

Gianluigi Ciacci

È avvocato specializzato nel diritto delle nuove tecnologie, dottore di ricerca presso l'Università degli studi di Roma "La Sapienza" in "Informatica giuridica e Diritto dell'Informatica" (1997), professore titolare delle cattedre di "Informatica Giuridica", di "Diritto Civile dell'Informatica" e di "Legal Aspects of Information Technology" presso la Facoltà di Giurisprudenza della "LUISS Guido Carli" di Roma, e della cattedra di "Informatica Giuridica: e-juris" presso la Facoltà di Giurisprudenza dell'Università "Link Campus University" di Roma. Autore di numerose pubblicazioni, tra cui le monografie "La firma digitale" (in tre edizioni, 1999-2002) e "Privacy e sanità" (2006) e i recenti saggi "Pagamenti elettronici e Moneta elettronica", (2012) e "Le fonti del diritto dell'informatica" (2011), dal 1996 è direttore editoriale del sito giuridico "Jei - Jus e internet", sul web di Internet all'indirizzo <http://www.jei.it>.

E-mail: studiociacci@jei.it

Giuseppe Corasaniti

Magistrato ordinario, Sostituto Procuratore Generale presso la Corte Suprema di Cassazione, è autore di numerosissimi studi in tema di diritto dell'informazione e dell'informatica. Docente in *Informatica giuridica*, presso il Dipartimento di Informatica, Facoltà di Scienze matematiche, fisiche e naturali dell'Università di Roma "La Sapienza". Docente di *Diritto penale dell'informatica* presso l'Istituto Superiore di Polizia, di *Diritto penale della comunicazione e dell'informatica* presso la Scuola di Polizia Tributaria della Guardia di Finanza. Docente di *Diritto penale e criminologia informatica* presso il Master di II livello in Scienze Forensi dell'Università degli Studi di Roma "La Sapienza" I Facoltà di Medicina e Chirurgia. È componente del Comitato Scientifico della Polizia Postale delle Comunicazioni. È stato consulente del Ministro per le politiche comunitarie in materia di comunicazione interattiva e politiche culturali nell'ambito della struttura di missione presso l'Unione Europea e Presidente del Comitato consultivo per il diritto d'autore presso il Ministero per i Beni e le attività culturali. È referente informatico per il distretto della Corte d'appello di Roma. Delegato dal Governo Italiano (ministero della Giustizia) e dall'Autorità per le garanzie nelle comunicazioni ai lavori del gruppo G8 a Berlino sul tema *Security and confidence in Cyberspace- Berlino 26/28 ottobre 2000*. Delegato dall'Autorità per le garanzie nelle comunicazioni, nella delegazione italiana del gruppo G8 sul tema *Security and confidence in Cyberspace-data retention group Tokyo 22/24 maggio 2001*. Delegato dall'Autorità per le garanzie nelle comunicazioni al workshop "*Information security in a networked world*" Tokyo 12/13 settembre 2001 organizzato dall'OCSE, dal Governo del Giappone e dall'IPA *Information-technology Agency* del Giappone.

E-mail: giuseppe.corasaniti@giustizia.it

Antonio Maria D'Amico

Importante ed articolata esperienza professionale in ambito italiano, europeo ed a livello di Commissione Europea. Dopo un breve periodo in Commissione a Bruxelles nella Direzione Generale Ricerca, Antonio è entrato a far parte dal 1990 al 1996 della Divisione Telecomunicazione di Price Waterhouse (ora PWC) per la quale ha operato prima a Bruxelles nell'ufficio Europa e successivamente a Parigi nella Divisione Enti locali; in questo ruolo ha maturato una profonda esperienza del mondo degli Enti locali francesi a livello centrale e locale. Nel 1996 Antonio ha creato la società European Business Associates Srl, (EBA) della quale è stato partner sino al 2012, che ha operato nel mercato della consulenza per l'internazionalizzazione delle imprese ed i finanziamenti comunitari. Dal 2001 al 2010 Antonio ha fatto parte del Gruppo tedesco Deutsche-Telekom (DT), come Amministratore Delegato della Società Eutelis Consult Italia, società controllata da Detecon, società di consulenza di DT, che ha operato con T-Systems in Italia.

E-mail: antoniomaria.damico@yahoo.it

Wanda D'Avanzo

Avvocato e dottore di ricerca in Filosofia del diritto presso l'Università degli studi di Napoli Federico II. È docente a contratto di Filosofia del diritto presso la Facoltà di Giurisprudenza dell'Università Telematica Unitelma-Sapienza di Roma. Presso la medesima Facoltà collabora

con la cattedra di Informatica Giuridica. È coordinatrice della Sezione territoriale per la Regione Calabria dell'Associazione Nazionale Docenti di Informatica Giuridica e Diritto dell'Informatica. Si è occupata della formazione giuridico-amministrativa dei pubblici dipendenti nell'ambito di progetti di attuazione e sviluppo degli sportelli unici per le attività produttive in Calabria. È autrice di diverse pubblicazioni sulle Riviste "Innovazione e diritto" e "Diritto e giurisprudenza agraria, alimentare e dell'ambiente". È, altresì, autrice delle seguenti monografie: "L'e-government", Movimedia, Lecce, 2007; "Partecipazione, democrazia, comunicazione pubblica. Percorsi di innovazione della Pubblica Amministrazione digitale", Rubbettino, Soveria Mannelli, 2009; "Il sistema dei controlli nelle amministrazioni pubbliche", Clioedu, Lecce, 2011. E-mail: wanda.davanzo@unitelma.it

Sandro Di Minco

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

Pasquale Luigi Di Viggiano

Ph.D. in Scienze Giuridiche. Attualmente professore a contratto di *Teoria generale dello Stato dell'Università* del Salento. Esperto di informatica giuridica, di metodologia della ricerca sociale e di sociologia del diritto. Si occupa dello studio delle periferie della modernità, della loro organizzazione sociale in relazione al diritto, alle teorie organizzative e al diritto della comunicazione digitale. E' impegnato nello studio dello Stato digitale e della sua struttura sistemica. Già

professore a contratto nell'Università telematica TELMA-LA SAPIENZA di Roma, titolare degli insegnamenti di *Sociologia della comunicazione elettronica* e di *Sistemi informativi nelle pubbliche amministrazioni*. Tra le sue pubblicazioni più recenti: *The Digital Public Administration. Legal rules and organizational models*, in «Curentul Juridic», Anno IX, n. 4 (47), 2011, pp. 19-44; *La formazione partecipata* (con F. Bochicchio), Guerini Editore, Milano 2012.

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

Fernanda Faini

Laureata con lode in Giurisprudenza presso l'Università degli Studi di Firenze, ha conseguito il Master universitario di secondo livello in Management Pubblico ed E-Government presso l'Università del Salento. E' responsabile dell'assistenza giuridica e normativa in materia di amministrazione digitale, innovazione, semplificazione, open government e sviluppo della società dell'informazione presso Regione Toscana. Collabora come docente in materia di diritto delle nuove tecnologie e amministrazione digitale con l'Università degli Studi di Firenze, dove è cultore della materia "Informatica giuridica". Collabora come docente con Formez PA e altre realtà. Autrice di pubblicazioni scientifiche e relatrice in convegni, conferenze e seminari in materia. Autrice di articoli di aggiornamento e approfondimento su quotidiani e riviste giuridiche online. Componente del Comitato di redazione della rivista "Il Documento Digitale". Blogger di Pionero - Digital Innovation, progetto di Maggioli editore. Membro di associazioni nazionali che si occupano di innovazione e diritto delle nuove tecnologie (Circolo dei Giuristi Telematici - CGT, Associazione Nazionale Docenti Informatica Giuridica e Diritto dell'Informatica - ANDIG, Società Italiana di Informatica Giuridica - SIIG e Rete per l'Eccellenza Nazionale - RENA).

E-mail: fernandafaini@gmail.com

Vittorio Frosini (Catania, 1922 – Roma, 2001)

Professore ordinario (dal 1971) ed emerito di Filosofia del diritto, Facoltà di Giurisprudenza, Università di Roma La Sapienza. E' considerato il padre dell'Informatica giuridica in Italia; fondatore della Associazione Nazionale Docenti di Informatica Giuridica (ANDIG). È stato componente laico nominato dal Parlamento del Consiglio Superiore della Magistratura (1986) e consulente dell'OCSE sulla regolamentazione dell'informatica. Ha presieduto l'Istituto di Teoria dell'interpretazione e di informatica giuridica - Facoltà di Giurisprudenza dell'Università di Roma La Sapienza. L'opera fondamentale è la *Struttura del diritto* (1962). In questa sede ricordiamo in particolare alcuni tra i saggi più importanti sul rapporto tra tecnologia e diritto: *Cibernetica: diritto e società*, 1968; *Il diritto nella società tecnologica*, Milano, Giuffrè, 1981; *Informatica, diritto e società*, 1988, Giuffrè; *Il giurista e le tecnologie dell'informazione*, 1988, Roma, Bulzoni; *L'automazione elettronica nella giurisprudenza e nell'Amministrazione Pubblica*, 1973; *La giuritecnica: problemi e proposte*, 1975; *Giustizia e informatica*, 1977; *La protezione della riservatezza nella società informatica*, 1981; *Riflessioni sui contratti d'informatica*, 1996; *Il giurista nella società dell'informazione* (2000). Rinviamo per tutta l'opera di Frosini al volume di Roberto Russano, *Vittorio Frosini. Bibliografia degli scritti (1941-1993)*, Milano, Giuffrè, 1994.

Tommaso Edoardo Frosini

Docente di Diritto pubblico comparato e di Diritto costituzionale nella Facoltà di Giurisprudenza dell'Università Suor Orsola Benincasa di Napoli dal 2007. È stato componente del comitato direttivo dell'Associazione Italiana dei Costituzionalisti, e attualmente è componente del direttivo dell'Associazione Italiana di Diritto Comparato. È stato componente di numerose commissioni ministeriali per la predisposizione di disegni di legge (in materia di: testo unico ambientale, riforma costituzionale, pari opportunità, redazione degli atti normativi). È stato componente della "Commissione di garanzia di attuazione della legge sullo sciopero nei servizi pubblici essenziali". È componente del Consiglio d'Amministrazione della Cassa di Risparmio di Rieti SpA. È condirettore della rivista *Munus. Rivista giuridica sui servizi pubblici*, vicedirettore della rivista *Diritto pubblico comparato ed europeo* e coordinatore della rivista *Percorsi Costituzionali*. È autore di oltre un centinaio di saggi apparsi sulle maggiori riviste giuridiche italiane, e dei volumi: *Sovranità popolare e costituzionalismo*, ed. Giuffrè, Milano, 1997; *Forme di governo e partecipazione popolare*, ed. Giappichelli, Torino, 2002 (terza edizione ampliata, 2008); *Le votazioni*, ed. Laterza, Roma-Bari, 2002; *Corso di diritto costituzionale*, ed. Cedam, Padova, 2007 (seconda edizione rivista, 2008); *Teoremi e problemi di diritto costituzionale*, ed. Giuffrè, Milano, 2008; *The Gamble of Fiscal Federalism in Italy*, Forum of Federation, Ottawa, 2010; *La lotta per i diritti. Le ragioni del costituzionalismo*, Edizioni Scientifiche Italiane, Napoli, 2011.

E-mail: tefrosini@gmail.com

Paolo Galdieri

Avvocato Cassazionista, Docente di Informatica Giuridica presso la Facoltà di Giurisprudenza dell'Università Luiss - Guido Carli. Coordinatore didattico del Master di II Livello in "Diritto dell'Informatica e Teoria e Tecnica della Normazione" presso l'Università degli Studi, La Sapienza di Roma. Già Docente di Diritto Penale dell'Informatica presso la facoltà di Economia dell'Università degli Studi di Chieti - Pescara, "G. D'Annunzio" e presso la Facoltà di Giurisprudenza dell'Università Luiss, Guido Carli di Roma. Già Professore a contratto integrativo presso l'insegnamento di Abilità Informatica della Facoltà di Giurisprudenza dell'Università degli Studi - "Federico II" di Napoli. Già Professore a contratto di Diritto Penale e Diritto Processuale Penale, Facoltà di Giurisprudenza, Università Telematica Unitelma Sapienza. E' stato Docente di Diritto Penale dell'Informatica presso numerosi corsi di perfezionamento e Master presso le Università di Chieti - Pescara, "G. D'Annunzio", Facoltà di Economia, Università LUMSA di Roma, Università di Lecce. E' autore di più di cinquanta pubblicazioni in materia di Diritto Penale dell'Informatica, tra lei quali la monografia *Teoria e Pratica nell'interpretazione del reato informatico*, Giuffrè, Milano, 1997. Nel 2005 ha redatto per conto dell'Unione Europea un rapporto sulla legislazione e prassi giudiziaria in materia di reati informatici in Italia, rapporto incluso nel "Handbook of legislative procedures of computer and network misuse in EU countries". Ha partecipato a Quito (Ecuador) nell'ottobre del 2001 al "I Congreso Mundial de Derecho Informatico" con una relazione dal titolo: "Il delitto informatico nella prassi giudiziaria". Unico rappresentante europeo al convegno sulla cyber criminalità tenutosi alla UAE University di Dubai (Emirati Arabi Uniti) il 24 novembre 2010 con una relazione dal titolo *Italian Criminal legislation concerning ICTs*.

E-mail: paolo.galdieri@tiscali.it

Donato A. Limone

Ordinario di informatica giuridica e docente di scienza dell'amministrazione digitale e di comunicazione pubblica, Università telematica Unitelma SAPIENZA, Roma. Presidente di ANDIG (Associazione Nazionale Docenti di Informatica Giuridica e diritto dell'informatica – www.andig.it). Fondatore e direttore della “Rivista elettronica di diritto, economia, management” (www.clioedu.it).

E-mail: donato.limone@gmail.com; donato.limone@unitelma.it

Andrea Lisi

Coordinatore del Digital&Law Department dello Studio Legale Lisi (www.studiolegalelisi.it), Presidente della Associazione Nazionale per Operatori e Responsabili della Conservazione digitale dei documenti (ANORC), Segretario Generale di AIFAG (Associazione Italiana Firma elettronica Avanzata e Grafometrica), Fondatore e Coordinatore degli Stati Generali della Memoria Digitale. Già Docente di Informatica Giuridica nella Scuola di Professioni Legali, Facoltà di Giurisprudenza dell'Università del Salento, oggi è docente nella Document Management Academy, SDA Bocconi, Milano, al MIS Academy - Management Information System – SDA Bocconi – IBM, nel IS Legal, SDA Bocconi, nel Master in Management della cultura digitale, editoria, archivi e biblioteche nell'era del 2.0, Università di Verona, di UniDOC - Progetto di formazione continua in materia di documentazione amministrativa, amministrazione digitale, delibere degli organi e documenti informatici - COINFO - Consorzio interuniversitario sulla formazione - Università degli Studi di Torino e nel Master “Esperto giuridico per l'Azienda Sanitaria” - promosso, per iniziativa di ALTEMS (Alta Scuola di Economia e Management dei Sistemi Sanitari), dalla Facoltà di Economia e dalla Facoltà di Medicina e Chirurgia dell'Università Cattolica del Sacro Cuore, in collaborazione con il Policlinico Universitario “A. Gemelli”. Ha fondato il Centro Studi&Ricerche Scint www.scint.it e la prima banca dati sul diritto dell'informatica www.scintlex.it. È stato Direttore della “RIVISTA DI DIRITTO ECONOMIA E GESTIONE DELLE NUOVE TECNOLOGIE”, Nyberg Editore, Milano e attualmente dirige la Collana “DIRITTO, ECONOMIA E SOCIETÀ DELL'INFORMAZIONE”, Cierre Edizioni, Roma. Oggi è direttore scientifico della rivista DMS (Document Management System) edita da Edisef e direttore editoriale della rivista IL DOCUMENTO DIGITALE pubblicata da Lex et Ars.

Attualmente è arbitro di numerosi enti di risoluzione stragiudiziale delle dispute relative ai domini Internet ccTLD.it, è Esperto Valutatore IMQ per il servizio di attestazione Q&S_CS (Qualità e Sicurezza nella Conservazione Sostitutiva) e collabora in tutta Italia con università, enti camerali, centri di ricerca, primarie società fornendo progettazione, formazione, assistenza e consulenza legale nell'e-business internazionale, nella privacy, nei servizi di conservazione digitale/fatturazione elettronica, nella realizzazione dei modelli organizzativi D. Lgs. 231/2001 e nel diritto delle nuove tecnologie, in genere.

E-mail: andrealisi@studiodl.it

Marco Mancarella

Professore aggregato di Informatica giuridica e Informatica della P.A. presso l'Università del Salento. Laureato in Giurisprudenza presso la LUISS Guido Carli di Roma. Vice Di-

rettore del Laboratorio di ricerca sull'eGovernment e Direttore del Master di II livello in Management pubblico e eGovernment del medesimo Ateneo. Componente del Consiglio Direttivo dell'Associazione Nazionale dei Docenti di Informatica Giuridica e di Diritto dell'Informatica(ANDIG). Componente del Consiglio Direttivo ANORC e Associato Fondatore di ANORC Professioni. Autore di numerosi lavori pubblicati in congressi, libri e riviste nazionali e internazionali. Visiting professor in tema di Amministrazione digitale presso Atenei in Francia e Grecia. Nell'ottica di un'avviata collaborazione con vari enti pubblici e aziende di settore, osservatore internazionale per i processi di eVoting.

E-mail: marco.mancarella@unisalento.it

Michele Melchionda

Laureato in Scienze dell'Amministrazione e Master in "Governance, Management, e-Government delle Pubbliche Amministrazioni". Esperto nella gestione e conduzione di infrastrutture tecnologiche e nella erogazione di servizi IT, è attualmente Dirigente Responsabile del Centro unico servizi della Corte dei conti presso la DGSIA. Tra i progetti di spicco seguiti per conto del settore pubblico in sinergia con i principali player tecnologici si annoverano progetti di consolidamento infrastrutturale, gestione data center e disaster recovery, sicurezza, collaborazione e gestione documentale, implementazione di architetture orientate ai servizi.

E-mail: michele.melchionda@corteconti.it

Marina Pietrangelo

Ricercatrice del Consiglio Nazionale delle Ricerche (CNR) presso l'Istituto di Teoria e Tecniche dell'Informazione Giuridica (ITTIG), dove è responsabile della Sezione di studi e ricerche in tema di diritto dell'informatica. È condirettrice della Rivista Informatica e diritto.

E-mail: pietrangelo@ittg.cnr.it

Irene Sigismondi

Ph.D. è avvocato cassazionista e collabora alle attività di ricerca dell'Università La Sapienza di Roma e Unitelma Sapienza nell'ambito delle problematiche legate all'interpretazione ed applicazione delle innovazioni, sia tecnologiche che giuridiche, sul mondo del diritto.

Ha svolto attività di ricerca con il CNR (IRSIG Bologna) e con lo YCIS dell'Università di Yale, USA, focalizzando gli studi sull'impatto delle tecnologie per la giustizia. Attualmente svolge attività di consultant per la Luiss Business School nell'ambito dei progetti Best Practices per gli uffici giudiziari italiani, finanziati su bandi regionali con fondi FSE.

E' co-coordinatore didattico del modulo sulla Teoria e Tecnica della Normazione per il Master in Diritto dell'Informatica della Sapienza e docente di abilità informatiche e telematiche.

Ha pubblicato una monografia sul buon andamento nella pubblica amministrazione (2011) ed uno studio provvisorio sull'informatizzazione della giustizia (2012), oltre a diversi articoli su vari temi più strettamente giuridici.

E-mail: irene.sigismondi@gmail.com

Giancarlo Taddei Elmi

Già dirigente di ricerca presso il Consiglio nazionale delle ricerche è attualmente associato all'Ittig, professore a contratto di informatica giuridica presso la Facoltà di Giurisprudenza di Firenze dal 1997 a oggi. Ha insegnato informatica giuridica presso l'Università Cattolica (Milano), Statale di Milano e presso l'Università di Cagliari. È stato professore a contratto di informatica giuridica anche presso la Facoltà di Scienze Politiche di Firenze. Ha tenuto numerose relazioni presso seminari e convegni nazionali e internazionali. Ha svolto attività di ricerca dal 1970 presso il CNR, con interessi verso l'informatica giuridica e il diritto dell'informatica. Pubblicazioni principali: Informatica e ordinamento giuridico, Giuffrè, Milano, 1988, Dimensioni dell'informatica giuridica, Liguori, 1990, I diritti dell'intelligenza artificiale tra valore e soggettività: fantadiritto o ius condendum?, Giuffrè Milano del 1990, pp.685-711, Logos e intelligenza artificiale, Adriatica 1999, Abilità informatiche per il diritto, Giuffrè, Milano 2006, Formazione giuridica e innovazione informatica, in Informatica e diritto, 1-2, 2008, 545-565, Il processo telematico, Informatica e diritto, ESI, 1-2, 2007, pp. 500 con ivi Introduzione. Dal processo telematico alla giurisdizione informatica p. 11-20, Corso di informatica giuridica, Napoli, Simone Editore 2010.

E-mail: giancarlo.taddei@ittg.cnr.it

Giampaolo Teodori

Avvocato; master in Diritto dell'Informatica e delle Nuove Tecnologie; ricercatore Formez Pa. Esperto di Diritto Amministrativo, di Pubblico Impiego e Responsabile di Progetti di Formazione e Selezione del Personale della P.A. Docente di "E-Government e Lavoro Pubblico" nel Master "Governance, Management, eGovernment delle PA", Università Unitelma Sapienza. E' stato professore a contratto presso la Scuola di Specializzazione per le Professioni Legali della Università di Salerno e docente su vari Master, da ultimo nel Master in "Management Pubblico ed E-Gov", Università del Salento. Autore di monografie e articoli in materia di E-Gov e di Pubblico Impiego. Relatore in convegni e conferenze su tematiche della Pubblica Amministrazione e dell'Innovazione.

E-mail: gteodori@formez.it

Angela Viola

Angela Viola, avvocato e dottore di ricerca in Informatica Giuridica e Diritto dell'Informatica, è docente dal 2000 presso l'Università degli Studi di Roma La Sapienza già al Corso di Perfezionamento in Informatica Giuridica e dal 2002 al Master Universitario II° Livello in Diritto dell'Informatica e Teoria e Tecnica della Normazione e presso l'Università Telematica Telma (Unitelma) al corso di diritto commerciale (dal 2005 al 2008). L'interesse accademico e professionale si concentra sulle tematiche di diritto e commercio elettronico, tutela del consumatore nei contratti a distanza e comunicazioni commerciali anche con esperienze di ricerca all'estero (School of Law Boston University USA, 1997). È componente del consiglio direttivo dell'ANDIG (Associazione Nazionale Docenti Informatica Giuridica).

E-mail: angelaviola@virgilio.it

L'ISTITUTO DI TEORIA DELL'INTERPRETAZIONE E DI INFORMATICA GIURIDICA DELL'UNIVERSITÀ “LA SAPIENZA”

Vittorio Frosini

Presentazione di
Tommaso Edoardo Frosini

I curatori di questo volume avevano inizialmente chiesto a me di scrivere un contributo sulla nascita e il consolidamento dell'Istituto di Teoria dell'interpretazione e informatica giuridica nella Facoltà di giurisprudenza dell'Università “La Sapienza” di Roma. Istituto che mio Padre ha fondato e diretto per un decennio, facendo rivivere, come una sorta di araba fenice, l'Istituto che Emilio Betti aveva creato nel 1955 (fino al 1960), ma aprendolo verso il futuro degli studi giuridici con l'aggiunta della denominazione “informatica giuridica” insieme alla “teoria dell'interpretazione”.

Ho esitato prima di rinunciare all'affettuoso invito che mi era stato rivolto. Ho esitato, perché forte era la tentazione di provare a rievocare quell'esperienza che mio Padre visse con grande entusiasmo e appassionato impegno. E mi sarebbe piaciuto raccontare come quell'entusiasmo e quell'impegno veniva avvertito a casa, in famiglia. Infatti, talvolta attraverso il “lessico familiare” si riesce a spiegare meglio la vita pubblica degli intellettuali, e quindi: perché hanno scritto quei libri, perché hanno assunto quelle posizioni, perché hanno sostenuto determinate tesi e fondato teorie. Se poi, com'è il mio caso, i figli hanno seguito le orme paterne, allora quanto si è appreso e imparato a casa, nelle abitudini quotidiane con il proprio genitore, diventa davvero determinante per la propria formazione, sia pure non subito ma a distanza di anni.

Mi sarebbe piaciuto raccontare, ma proprio per questo ho preferito non farlo. Primo, perché mi avrebbe fatto velo l'affetto filiale e avrei ceduto a un racconto tendenzialmente agiografico; secondo, perché l'esperienza dell'Istituto di Teoria (come veniva chiamato) non l'ho vissuta direttamente, provenendo e formatomi in un altro Istituto universitario, quello di Teoria dello Stato e istituzioni politiche comparate. E allora, avrei fatto torto a quel gruppo di allievi e amici di mio Padre che con lui hanno vissuto, con pari entusiasmo e con grande impegno, l'avventura dell'Istituto di Teoria, e che sono tutti evocati nel contributo di mio Padre appreso ristampato. Ho pensato, infatti, che la cosa migliore fosse far “rivivere” un saggio che mio Padre scrisse per il decennale di vita dell'Istituto di Teoria, in occasione di uno dei tanti e importanti convegni che l'Istituto organizzò nel corso della sua attività, dove si racconta la nascita dell'Istituto, il collegamento fra la Teoria dell'interpretazione e il diritto informatico e si svolgono delle considerazioni sugli sviluppi delle tematiche. Mi è sembrato, e spero che il lettore converrà con me, che la ripubblicazione di questo saggio, apparso soltanto in un volume, il tredicesimo della collana dell'Istituto (Esperienze giuridiche del '900, a cura di F. Modugno, Milano, Giuffrè, 2000) fosse la scelta migliore. Certo, rimangono fuori tante storie che si legano all'Istituto di Teoria, al suo direttore e agli

studiosi che hanno avuto la ventura di frequentarlo. Ognuno di loro, citando Proust, potrebbe dire che “i ricordi dei luoghi che amiamo altro non è che il ricordo delle ore felici, che vi abbiamo vissute”.

Una cosa però è doverosa dirla: l’Istituto frosiniano è stato il primo, in Italia, a far vivere l’informatica giuridica dentro una Facoltà di giurisprudenza; così come è stato il primo a fondare un corso di perfezionamento e un dottorato di ricerca in informatica giuridica e diritto dell’informatica, creando e diffondendo una cultura del diritto nella società tecnologica. Non poteva non essere così, da parte di chi era stato il primo in Italia, e tra i primi in Europa, nel lontano 1968, a scrivere “Cibernetica, diritto e società”.

La teoria dell’interpretazione giuridica e del diritto informatico: uno sguardo sul presente

1. Dieci anni or sono ebbe inizio l’attività dell’Istituto di teoria dell’interpretazione e di informatica giuridica, con la riunione di insediamento del Consiglio dell’Istituto l’11 novembre 1987. Esso era stato creato con una delibera della Facoltà di giurisprudenza in data 13 ottobre 1986, con l’intento di ridare vita e rimettere in funzione l’Istituto di teoria dell’interpretazione, che era stato fondato da Emilio Betti nell’ottobre 1955 e da lui diretto fino al suo collocamento fuori ruolo nel novembre 1960. A Betti si deve altresì l’istituzione della cattedra omonima, che egli tuttavia ricoprì per incarico: fu solo nel 1986 che ad essa venne chiamato un professore ordinario della materia, dunque il primo titolare *pleno jure* della nuova disciplina nell’università italiana. Il mutamento della denominazione dell’Istituto fu significativo di un suo nuovo aspetto. Anzitutto, il compito di ricerca e di insegnamento, che per Betti era comprensivo delle varie forme di ermeneutica culturale, come mostra la sua nota opera *Teoria generale dell’interpretazione*, venne ristretto alla interpretazione del diritto. Inoltre, l’Istituto acquisì una nuova dimensione di lavoro intellettuale, quella dell’informatica giuridica; per cui esso venne in seguito accresciuto con i corsi di dottorato di ricerca e con un corso di perfezionamento in questa materia. L’Istituto fu così dotato di una adeguata ed aggiornata attrezzatura tecnologica per assolvere ai suoi nuovi compiti, e la sua dotazione ed organizzazione venne curata in questo campo, con competenza e dedizione, da Gianfranco Caridi. Nella sua ricerca nel campo dell’interpretazione giuridica il direttore venne coadiuvato, con un contributo continuo di lucida ed appassionata intelligenza, da Francesco Riccobono; ai due ricercatori ora ricordati si aggiunse in seguito Anna Jellamo, che estese l’indagine ermeneutica al campo della filosofia politica e della dottrina dello Stato, con risultati originali e significativi.

Tutti e tre hanno pubblicato i loro lavori, di alto interesse e di sicuro valore scientifico, nella collana editoriale dello stesso Istituto; nella quale sono stati accolti anche volumi di autorevoli colleghi come Enzo Sciacca, di giovani studiosi come Paolo Galdieri, e importanti ristampe di classici come le opere di Max Ascoli – con l’apporto di due saggi di Renato Treves, indimenticato Maestro – e di Emilio Betti, in una nuova edizione curata da Giuliano Crifò; allo stesso Betti, fondatore dell’Istituto, è stato dedicato un convegno di studi, i cui Atti sono stati pubblicati nella collana. Alla quale si sono affiancate successivamente la serie dei *Quaderni di ricerca e di documentazione* e la nuova collana di ricerche sull’interpretazione del diritto costituzionale,

curata dall'attuale titolare della cattedra, con la collaborazione degli allievi legati al suo magistero: mi riferisco a Franco Modugno.

Merita ricordare, che nell'ambito dell'attività dell'Istituto si è svolta anche quella dell'ANDIG, l'Associazione nazionale dei docenti di informatica giuridica, che ha avuto la sua sede presso lo stesso Istituto, che si è giovata dell'opera del suo Segretario generale, Donato Limone, e che ha dato vita ad una collana di studi e ad iniziative di convegni, di interesse specifico per la disciplina del diritto informatico. L'Istituto ha promosso ed ospitato anche convegni e conferenze di vario argomento ermeneutico, ai quali hanno preso parte illustri studiosi italiani e stranieri. Basti qui fare riferimento ad un nome solo ma altamente rappresentativo: quello di Hans Gadamer.

Il compito di guidare l'attività scientifica, didattica ed organizzativa è toccato al direttore dell'Istituto. Del suo impegno fanno fede le *Lezioni di teoria dell'interpretazione giuridica*, pubblicate in forma ciclostilata nel marzo 1989, e giunte negli anni seguenti alla quinta edizione con accrescimenti. Il loro contenuto teorico è confluito nella opera dello stesso autore apparsa in lingua tedesca nel 1995 col titolo *Gesetzgebung und Auslegung*, preceduta da una presentazione di Erhard Denninger; una traduzione parziale in lingua spagnola delle Lezioni era già apparsa nel 1991, col titolo di *Teoría de la interpretación jurídica*.

Cessato l'Insegnamento cattedratico, le idee esposte in dieci anni sono state rielaborate in forma nuova ed unitaria nel libro intitolato *La lettera e lo spirito della legge*, apparso in prima edizione nel 1993 e in una seconda edizione nel 1995: nello stesso anno esso venne pubblicato in lingua spagnola, *La letra y el espíritu de la ley*, con un *Pròlogo* di Carols Alarcòn Cabrera. È a questo volume che si può fare riferimento per segnare il punto della navigazione intellettuale nel pelago della metodologia interpretativa del diritto e per gettare uno sguardo sulla situazione attuale.

2. Dieci anni or sono, la cultura giuridica italiana appariva ancora dominata, in materia di teoria dell'interpretazione, dalla presenza e dalla influenza di due opere, quella di Emilio Betti sulla *Interpretazione della legge e degli atti giuridici*, della quale una edizione riveduta ed ampliata a cura di Giuliano Crifò era apparsa nel 1971, e quella di Giovanni Tarello, *L'interpretazione della legge*, pubblicata nel 1980. Non erano queste, beninteso, le sole esistenti sul mercato delle idee: saggi e libri di teoria dell'interpretazione erano succeduti l'uno all'altro fin dall'inizio del secolo attuale, arando un terreno fecondo per la crescita delle due opere ricordate. Ho tracciato le linee portanti di questa vicenda culturale nella mia relazione, tenuta ad un convegno indetto dalla Facoltà giuridica di Catania nel giugno 1996, e pubblicata col titolo: *Dalla legislazione all'interpretazione: il caso italiano*; perciò non mi soffermo sul tema.

Sotto il profilo metodologico, il volume di Emilio Betti e quello di Giovanni Tarello appaiono come speculari l'uno all'altro. Betti, ispirato nella sua concezione dalla filosofia dell'idealismo ontologico e critico di Nicolai Hartmann, sosteneva che il procedimento ermeneutico condotto dal giurista sul testo di legge consiste nella instaurazione di un rapporto ideale fra lo spirito del legislatore e quello dell'interprete, il quale faceva così tornare la luce l'intenzione dell'autore della legge. Questa formulazione venne ironicamente paragonata da Uberto Scarpelli ad una evocazione spiritica da opera di un *medium*; giacché per Scarpelli, che era un seguace ed un originale rielaboratore della dottrina logico-analitica detta della Scuola di Oxford, l'analisi interpretativa andava condotta sul testo della legge come suo termine iniziale e finale, e consi-

steva in una riformulazione linguistica di quel testo. Come aveva già scritto Thomas Hobbes nel suo *Leviatano*, una legge non può avere che un solo significato valido, quello che è stato espresso nella sua lettera, con la quale fa tutt'uno l'intenzione della legge.

Questa stessa dottrina è stata sostenuta, sia pure con personali adattamenti, anche nell'opera di Giovanni Tarello, in scoperta polemica con la teoria di Betti, ed è condivisa ancor oggi da giuristi e da filosofi del diritto. Il recente volume di Michele Ainis, *Le parole e il tempo della legge*, del 1996, ricco di cultura e di acume, si apre con un capitolo intitolato *Due parole sulle parole della legge*, dedicato ad una garbata ma penetrante e ferma replica al libro già citato di *La lettera e lo spirito della legge*; replica in cui si riafferma "la soglia che divide il campo dell'interpretazione letterale da quella teleologica" in cui si spinge invece chi ricerca lo spirito della legge: giacché per Ainis la legge è tutta in se stessa, come appare nella sua espressione letterale. È questo il punto di vista, al quale si può dare il titolo di *textualism*, come viene definito e sostenuto da Antonin Scalia, uno dei giudici della Corte Suprema degli Stati Uniti, nel suo libro che è stato appena pubblicato col titolo: *A Matter of Interpretation. Federal Court and the Law*. E poiché il giudice Scalia decide, ovvero si contrappone con la sua *dissenting opinion*, nel merito dei giudizi espressi dalla più antica corte costituzionale, egli apporta alla dottrina, di cui Ainis si è fatto interprete teorico in Italia, un peso specifico di autorevolezza pratica indubbiamente rilevante. A questo orientamento di decisione giudiziaria stretta e ristretta alla lettera della legge si contrappone quello reso esplicito nell'art. 1 del codice civile svizzero: "la loi régit toutes les matières auxquelles se rapportant la lettre ou l'esprit de une de ses dispositions". Se il giudice Scalia sedesse in una corte svizzera, sarebbe tenuto a tener conto di un tale principio. E d'altronde, una revisione critica delle sentenze a cui ha preso parte è contenuta nel vivace libro di Robert Nagel, *Judicial Power and American Character*.

Tornando sul piano teorico, va riconosciuto che la concezione bettiana è condizionata da una premessa, che è difficile condividere. La ricerca dello spirito del legislatore è una ricerca vana: di quel legislatore originario molte volte non si conosce più l'identità storica, col passare degli anni e dei secoli che da lui ci dividono; i mutamenti sopravvenuti nelle situazioni politiche, nei costumi sociali, e nello stesso linguaggio legislativo rendono infruttuosa o ingannevole la ricerca delle intenzioni; e su tal punto i critici avversi ad una tale ricerca hanno ragione. Giacché il solo, il vero legislatore di cui il giudice (o il giurista in generale) deve farsi interprete è il legislatore attuale, non quello originario: giacché il legislatore, se mantiene in vigore una legge del passato, ha voluto così farla propria, le ha conferito legittimità e nuovo senso giuridico nel complesso del quadro normativo; altrimenti, egli l'avrebbe abolita o sostituita o modificata. Rimane aperto il problema, se vi sia, nelle parole della legge, da ricercare un significato, che sia funzionale per la decisione concreta da prendere sul caso posto in giudizio, che non era previsto dalla legge nella sua configurazione particolare; ovvero, per il quale la legge si palesa ambigua nella sua lettera.

3. Nella produzione scientifica di Emilio Betti è però contenuta una enunciazione della metodica giuridica dell'interprete, che non tutti i suoi commentatori hanno recepito, perché confinata nelle pagine di un suo breve *Corso di teoria generale del diritto*, pubblicato in francese in appendice al suo corso di diritto comparato delle obbligazioni, tenuto all'università del Cairo nell'anno accademico 1557-58. Betti vi afferma, che due sono le fonti del diritto: l'una, la legi-

slazione, l'altra, l'interpretazione e l'integrazione ad opera della giurisprudenza. Vi è, com'egli scrive, "un processo inesauribile di circolazione, che collega alla legislazione l'interpretazione che ne fanno la dottrina e la giurisprudenza". È chiaro, pertanto, che l'opera dell'interprete non si limita alla evocazione dello spirito del legislatore, ma che essa conferisce, alla morta lettera della legge – che è quella dettata dal legislatore, rimasta statica ed inerte nel tempo, racchiusa e conchiusa nella sua letteralità come in una bara –, il proprio spirito vivificatore. Per dirla con una frase, sintetica ma indicativa, la legge viene scritta per essere letta, viene letta per essere interpretata, viene interpretata per essere applicata.

Ho ricordato la critica avanzata da Michele Ainis come particolarmente significativa dell'interesse suscitato dalla rivendicazione di uno spirito della legge, proprio perché essa è una posizione dialettica rispetto all'altra. Si potrebbero però citare anche i numerosi interventi, da parte di studiosi italiani e stranieri, a favore della tesi contrastata. Senza qui farne un elenco, vorrei almeno ricordare tre nomi di studiosi, che hanno compiuto una lettura attenta e consapevole anche delle implicazioni, che la dottrina accennata comporta, e che sono i nomi di tre colleghi, a me assai vicini anche negli affetti: Franco Modugno, Massimo C. Bianca e Francesco Riccobono, autori di tre saggi critici sul mio libro già citato.

La tesi sostenuta in esso contiene delle implicazioni, di cui qui indicherò qualche svolgimento. La prima di esse è, che la legge non è soltanto un messaggio rivolto dal legislatore all'interprete, che deve osservarla e farla osservare, sia egli magistrato giudicante od esecutore amministrativo. La legge è anche una metafora verbale delle strutture dei comportamenti sociali, che devono essere tenuti, cioè agiti, dai soggetti. La legge rappresenta una morfologia della prassi sociale, essa è una maniera di leggere, in termini giuridici, cioè impositivi o permissivi, la realtà sociale a cui deve essere applicata: realtà che ad essa deve conformarsi o alla quale può anche sottrarsi o ribellarsi, ma che comunque rappresenta una griglia interpretativa della realtà. Il giudice quando legge ed interpreta il testo di una legge, al contempo legge ed interpreta attraverso il testo di legge il comportamento da giudicare, valendosi dello schema contenuto in quel testo come elemento di ricostruzione e valutazione della fattispecie, attuando una conversione del vero col fatto.

L'altra dimensione, in cui trova sviluppo la dicotomia fra la lettera e lo spirito della legge, è quella relativa al rapporto fra i principi e le norme, cioè fra l'intento regolativo della legge e la sua esplicazione semantica. La legge non consiste nell'insieme delle norme, giacché la norma non è che una componente di essa, l'altra componente è il principio che la anima, il valore di legalità che la giustifica. Erroneo è dunque il vecchio detto, *quod non est in lege, nec in iure*: giacché il diritto è il contesto in cui è inserito il testo di una legge, è l'insieme dei principi che reggono un ordinamento giuridico, ne assicurano la coerenza e la continuità, che trovano adesione ed applicazione nel giudizio dell'interprete.

Ancora una implicazione va rilevata nel riconoscimento del rapporto dialettico esistente fra la lettera e lo spirito della legge: essa è quella del rapporto che si instaura fra la coscienza del singolo giurista-interprete e la coscienza comune presente nell'ordinamento giuridico, di cui egli partecipa. È quella, che è stata chiamata la coscienza nomologica, la coscienza che si rispecchia, si riconosce, si completa nella coscienza più vasta di una comunità, superando il momento del confronto immediato con la singola proposizione di legge. Il giurista, e non solo il giudice, è soggetto alla legge; ma questa è anzitutto la Legge con la maiuscola, lo spirito della legge e non la sua lettera.

4. Vi è poi un equivoco da dissipare, in cui sono incorsi anche valenti studiosi. Il procedimento di interpretazione giuridica non è uno ed unico, non è un metodo unitario di analisi, ma è articolato in diverse specificazioni, e perciò non può ridursi alla semplice e semplicistica operazione analitica e ricompositiva del linguaggio di un testo di legge. Vi sono infatti tre forme principali di metodica interpretativa, diverse fra loro. La prima è quella messa in opera dallo stesso legislatore, quando egli emana una legge interpretativa di una sua legge precedente; la quale nuova legge va interpretata a sua volta, in relazione alla precedente. È sorta pertanto la questione, se si tratti di una legge retroattiva, che stabilisce certi effetti giuridici differenziati da quelli della legge precedente ma a quella li attribuisce, e che perciò valgono *ex tunc*, ovvero si tratti di una legge modificativa, i cui effetti valgono dunque *ex nunc*. Sebbene la questione sia controversa, si può fondatamente ritenere, che ogni legge è innovativa, che essa dispone dal momento della sua emanazione. La nuova legge, interpretando le disposizioni della legge cui si applica, attua quella integrazione ermeneutica che conferisce un significato alla legge interpretata.

La seconda forma di interpretazione è quella attuata dal giudice e che si differenzia dalla prima, perché non dispone in generale, ma con riferimento preciso e limitato alla fattispecie; almeno così avviene nei sistemi giuridici di impianto napoleonico sul continente europeo. Il giudice perciò si distingue dal legislatore, in quanto egli ne è l'interprete: ossia, la lettera della legge è la parola del legislatore, lo spirito della legge è la parola dell'interprete, che quella parola adatta al caso concreto, con un procedimento di dissezione e di ricomposizione delle norme, mai riducibili ad una sola, ma sempre in connessione fra loro.

La terza forma, da distinguersi dalle precedenti, è quella che viene messa in opera dal funzionario amministrativo, il quale manovra su un margine di discrezionalità, conferitagli nell'interesse pubblico. La dottrina amministrativistica ha messo in evidenza l'evoluzione avvenuta nella nozione dell'interesse pubblico, prima attribuito alla personalità giuridica dello Stato, poi riconosciuto alla comunità dei cittadini.

Vi sono poi delle forme secondarie di procedimento interpretativo nel diritto: una di queste è quella forense, di cui è stato addirittura contestato il carattere giuridico. Tuttavia, tale carattere le compete, giacché essa fa parte integrante della dialettica del processo e configura un ragionamento giuridico che costituisce un presupposto della sentenza. Anche all'interpretazione dottrinale è stato contestato il profilo giuridico che essa indubbiamente assume, riducendolo a quello culturale; ma va osservato, che le opinioni dei dottori della legge hanno avuto una funzione autoritativa in certi periodi storici, e che ce l'hanno ancora in certi ordinamenti giuridici con fondamento religioso. Si può aggiungere alla due forme citate anche quella notarile, seppure svolta nei suoi limiti, ma che è stata riconosciuta come tale dalla dottrina.

Si consideri infine la funzione interpretativa assolta dalle corti costituzionali, le quali si pongono al di sopra delle leggi stesse, e che giudicano appellandosi a principi che non sono enunciati in alcuna norma in senso letterale, come è per il principio di ragionevolezza. Il richiamo che esse fanno ai valori della carta costituzionale conferma il carattere contestuale che deve avere l'interpretazione giuridica, e si potrebbe dire che quella costituzionale è una forma interpretativa autonoma rispetto alle altre che sono state enunciate. Come si è accennato sopra, l'attività scientifica dell'Istituto si è aperta in anni recenti a questa prospettiva di ricerca con un sostanzioso contributo di studi raccolti in volume; ed io aderisco alla tesi di una specificità

della interpretazione costituzionale, modificando le opinioni espresse in precedenza sulla sua analogia a quella legislativa od a quella giudiziaria.

5. Non meno sorprendente delle rivoluzioni politiche, che hanno mutato la fisionomia dei regimi durante questi ultimi dieci anni, è stata la rivoluzione tecnologica, che ha provocato addirittura una mutazione antropologica, con la creazione dell'uomo artificiale, che si va sottraendo ai condizionamenti dell'ambiente naturale ed alle stesse leggi di natura, cui prima era soggetto il suo corpo. In questa sede, tuttavia, ci limiteremo ad illustrare soltanto gli aspetti relativi all'avvento della società dell'informazione automatizzata, in considerazione degli specifici compiti di ricerca e didattica di questo Istituto.

Dieci anni or sono non si era ancora diffuso l'uso del telefono cellulare, che si può prendere ad emblema del nuovo modo di vivere e di comunicare dell'uomo e della donna in una società industriale avanzata. Si noti, che il progresso nel campo delle telecomunicazioni aveva già abolito le distanze di trasmissione, prima con il telegrafo, poi con il telefono, la radio, la televisione e la telematica, riducendo sempre più anche i tempi di trasmissione fino alla contemporaneità. Con il telefono cellulare si presenta però un nuovo fenomeno di trasformazione. Anzitutto, il punto di trasmissione e di ricezione dei messaggi non è più un punto fisso, statico, come l'ufficio del telegrafo o l'impianto telefonico; esso è divenuto mobile, si sposta e diventa onnicentrico, ossia non è più collegato da punto a punto con un cavo, ma irradia e riceve il messaggio in e da ogni direzione. Inoltre, esso è personalizzato: chi chiama o risponde è sempre il suo portatore e non una terza persona, esso stabilisce non un domicilio ma un'identità, conferisce una nuova libertà individuale. Esso ha già avuto in Giappone un nuovo sviluppo qualitativo: ad esso è collegato uno schermo miniaturizzato, che consente di vedere l'immagine dell'interlocutore (o della interlocutrice) insieme al sentirne la voce.

Sotto il profilo giuridico della tutela della riservatezza si aprono perciò dei nuovi problemi: giacché potranno essere intercettate, registrate, memorizzate, elaborate e riprodotte non solo le parole e le voci, ma anche le immagini: un Grande Fratello, di orwelliana memoria, avrà orecchi e occhi più del mitico Argo. Al rischio del maleficio telematico, dovuto ad un abuso di potere, si contrappone tuttavia un evidente beneficio: l'uomo non sarà più solo in mezzo al mare, al deserto, alla foresta, vivrà nella quarta dimensione di uno spazio virtuale.

In quanto al computer, del quale il telefono cellulare è un derivato, in questi dieci anni esso è diventato il teleputer: inserito nelle autostrade elettroniche delle fibre ottiche, esso compone una sinergia dei vari mezzi di comunicazione tecnologica, e funziona anche da telefono, da televisore e da fax. Esso è divenuto anche il punto di raccordo fra le reti di trasmissione nel cyberspazio collegandosi con l'Internet, e si è creata così una nuova ed esaltante capacità umana di informazione, di comunicazione, di creazione intellettuale, estesa su tutto il pianeta, coscienza comune del genere umano.

L'altra grande novità verificatasi nel corso del decennio passato è stata quella dell'avvento della editoria elettronica. Era già quasi magico costringere una intera sinfonia od un'opera lirica nel breve spazio di un nastro di cassetta o su un disco di CDROM; è stata una conquista della intelligenza umana, che ha consentito di concentrare le informazioni anche in una biblioteca elettronica. Per la consultazione di dati giuridici oltre che collegarsi con una banca dati si può oggi accedere al testo di una legge, di una sentenza, di un commento valendosi della memoria

elettronica, superiore a quella di qualunque giurista. Questo fatto modifica la ricerca e la didattica del settore giuridico e rappresenta l'apertura di un nuovo spazio mentale. Tuttavia si possono avanzare alcune osservazioni.

Con il ricorso alla conoscenza ed alla consultazione elettronica, il discorso giuridico viene a perdere in continuità ed in compattezza, in quanto ogni testo viene sbriciolato e si perde la visione d'insieme, che derivava dalla lettura e dalla confidenza acquisita con l'alberatura delle norme e con la selezione non meccanica ma organica delle idee. L'automazione dell'informazione giuridica ha avuto i suoi effetti positivi e negativi anche sulla didattica: quando l'esame dello studente viene effettuato mediante il ricorso ai *tests* informatici, si guadagna tempo e si procede in maniera obiettiva, ma si sterilizza il rapporto fra il discente e l'esaminatore, e non sempre si ottiene il risultato di una valutazione adeguata delle capacità di un giovane: la sua risorsa dialettica, la sua partecipazione umana a certi problemi, la sua energia intellettuale; in una parola, la sua personalità. L'università di massa richiede comunque una gestione adeguata alla sua funzionalità, per cui la tessera elettronica ha sostituito il vecchio libretto delle frequenze e degli esami sostenuti, in cui le prime ed i secondi venivano convalidate dalla firma del professore.

6. Una particolare riflessione va indirizzata a quel settore del diritto, che riguarda le informazioni automatizzate e la loro trasmissione telematica, considerate non come strumenti ma come elementi di indagine e di giudizio: il diritto informatico, un termine questo che dovrebbe affiancarsi agli altri già accolti nell'uso di diritto aeronautico, di diritto spaziale, ecc.

Nel trascorso decennio si sono formate una legislazione ed una giurisprudenza, che non trovava posto nei manuali giuridici di dieci anni fa: a differenza dei vetusti schemi e problemi tramandati sin dagli inizi dell'ottocento, dopo la trasformazione subita dal diritto in Europa per l'impulso ricevuto dalla concezione imperiale napoleonica. L'Europa d'oggi ha ricevuto invece una poderosa spinta verso un nuovo orientamento politico e giuridico dalla formazione di una nuova economia dominata dai nuovi metodi elettronici di elaborazione e di trasmissione dei dati. Un'ampia ed articolata analisi dei nuovi problemi sottoposti all'attenzione dei giuristi è quella contenuta nel volume pubblicato da questo Istituto e intitolato *Problemi giuridici dell'informatica nel MEC*, curato da Paolo Galdieri. Non è vana vanteria affermare che l'Istituto ha tenuto sempre aperta una prospettiva culturale sull'Europa, documentata dai rapporti con altri centri di cultura giuridica informatica, italiani come il CIRFID di Bologna e stranieri come quelli di Londra e di Oslo. Conferenze, convegni, ricerche e pubblicazioni hanno conferito a questo Istituto un prestigio scientifico, che ha superato le frontiere del nostro Paese. Ricorderò rapidamente le tappe principali del percorso legislativo di questi anni in materia di informatica. Il 12 febbraio 1983 venne emanato il decreto legislativo n. 39, contenente le "Norme in materia di sistemi informativi automatizzati delle amministrazioni pubbliche", con il quale veniva istituita una Autorità per l'informatica nella Pubblica Amministrazione (AIPA). Il 23 dicembre 1993 seguì il decreto legislativo n. 547, con le norme modificatrici del codice penale e del codice di procedura penale in previsione dei reati informatici. Il 31 dicembre 1996 apparve finalmente la legge n. 675, dedicata alla "tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali", una legge che rompeva il sonnambulismo legislativo che durava dal 1981; con essa veniva istituito l'Ufficio del Garante per la protezione dei dati. A queste due Alte Autorità si è venuta ad aggiungere quella competente per le garanzie sui sistemi di telecomunicazioni

(legge del 31 luglio 1997, n. 249). Vi è dunque ormai piena materia di studio e di pratica per la creazione di un corpo di esperti, alla cui preparazione da anni si dedica questo Istituto.

7. Alla fine di questo convegno, che ha visto la partecipazione di illustri relatori e di un cortese ed attento pubblico di ascoltatori, giunge l'ora del saluto di congedo del direttore dell'Istituto. Ai collaboratori di questi dieci anni di attività va il mio profondo ringraziamento: a Gianfranco Caridi, a Francesco Riccobono e ad Anna Jellamo, che sono stati miei allievi ancor prima dell'inizio del nostro sodalizio di lavoro, e che sono divenuti parte della mia stessa vita, e non mi posso staccare da essi come dai muri, dai tavoli, dagli scaffali di questo Istituto; ed anche Laura Agostini, sopraggiunta in anni successivi, è divenuta parte integrante dei ricordi e degli affetti, che mi accompagneranno per il resto della mia vita. Il mio ringraziamento va esteso agli altri collaboratori, Brunella Talarico, Rosa Tozzi e Romualdo Bernardini, per la disponibilità e la cortesia sempre dimostrate nel loro impegno di lavoro. Vorrei ancora menzionare i nomi dei docenti Vittorio Novelli, Francesco Durante e Paolo Bisogno e degli allievi di corsi di dottorato di ricerca, dai quali ho ricevuto profonde soddisfazioni per i loro successi nel lavoro culturale e per le affermazioni ottenute anche nella vita civile, alle quali l'Istituto ha contribuito a prepararli. Ricorderò soltanto il nome di Paolo Galdieri, perché egli è stato anche in organico nell'amministrazione dell'Istituto. E infine, vorrei rivolgere il mio pensiero, memore ed affettuoso, ai miei colleghi della Facoltà, che mi chiamarono a coprire questo ufficio e che mi hanno confermato ogni anno nella direzione, accogliendo la designazione del Consiglio dell'Istituto, fin dall'ormai lontano 13 ottobre 1986: accomuno i loro nomi in uno solo, che li rappresenta nell'istituzione e nel sentimento di amicizia, il Preside della Facoltà Carlo Angelici.

L'ASSOCIAZIONE NAZIONALE DEI DOCENTI DI INFORMATICA GIURIDICA E DI DIRITTO DELL'INFORMATICA (ANDIG) DIARIO BREVE (1988-2013)

Donato A. Limone

Abstract: Un diario breve della fondazione, delle attività e della rinascita di ANDIG (1998-2013). L'Associazione ha svolto e svolge un ruolo importante per lo sviluppo del rapporto tra diritto e tecnologie dell'informazione.

Parole chiave: informatica giuridica; diritto dell'informatica; società dell'informazione; didattica.

Sommario: 1.Premessa. - 2.I docenti di Informatica Giuridica nel censimento del 1987 - 3.Il Convegno di Camerino sull'Insegnamento della Informatica Giuridica (1988)- 4 Metodologia dell'insegnamento del diritto con sussidi tecnologici: il convegno di Roma del 1991. - 5. I corsi di perfezionamento e di master attivati con il supporto dell'ANDIG. Il contesto universitario. - 6. L'Informatica giuridica oggi: il convegno ANDIG di Roma del 1.12.2005. - 7. Il nuovo statuto ANDIG del 2012: la rinascita. - 8. Il convegno di Roma del 29 ottobre 2013 "I nuovi scenari della società dell'informazione: aspetti politici, giuridici, amministrativi e tecnici".

1.Premessa

Questo breve appunto è una sorta di "diario" breve che registra i momenti più importanti dell'attività dell'ANDIG, dall'atto della fondazione ad oggi.

L'Associazione Nazionale dei Docenti di Informatica Giuridica viene istituita il 15 gennaio 1988 in Roma con l'obiettivo di contribuire allo sviluppo della disciplina di Informatica Giuridica e alla diffusione della cultura e delle professioni in materia di diritto e tecnologie dell'informazione. L'ANDIG nasce da una idea e da un progetto definito dai professori Vittorio Frosini (ordinario di Filosofia del diritto, Facoltà di Giurisprudenza, Università degli Studi La Sapienza, docente che per primo in Italia ha effettuato studi di informatica giuridica ed insegnato la stessa materia) e Donato A. Limone (nel 1985, primo docente di ruolo della disciplina, in qualità di associato presso la Facoltà di Giurisprudenza della Università degli studi di Camerino). Il 9.11.2012 l'ANDIG approva un nuovo statuto sulla base di un nuovo progetto di associazione che, senza modificare

l'acronimo, diventa l'Associazione Nazionale dei Docenti di Informatica Giuridica e di Diritto dell'informatica. Una storia di 25 anni di periodi di piena attività alternati a periodi lunghi di pausa. In questi anni l'ANDIG ha contribuito allo sviluppo della Informatica giuridica e del Diritto dell'informatica con un approccio che si è caratterizzato ora per "distinguere" tra Informatica giuridica e Diritto dell'informatica, ora per sfumare questa distinzione. Oggi l'Associazione ha raggiunto una posizione "matura": oggi si occupa di due approcci nell'ambito di una *unica area tematica* che si caratterizza per la interrelazione forte tra "diritto e tecnologie dell'informazione".

2.I docenti di Informatica Giuridica nel censimento del 1987

La cattedra di informatica giuridica dell'Università di Camerino (prof. Donato A. Limone) effettuò nel giugno del 1987 una indagine per rilevare quanti insegnamenti di informatica giuridica fossero stati attivati. L'indagine interessò 73 Facoltà di Giurisprudenza, Scienze Politiche, Economia e Commercio. Risposero 29 Facoltà. Su 29 Facoltà 13 avevano attivato corsi di Informatica Giuridica: 3 corsi nelle Facoltà di scienze politiche; 2 corsi nelle facoltà di Economia e commercio; 8 corsi nelle Facoltà di Giurisprudenza. I docenti erano 16: 15 a contratto; 1 professore di ruolo (Università di Camerino). Erano stati istituiti inoltre l'Istituto di Teoria dell'interpretazione e di informatica giuridica, Roma, Facoltà di Giurisprudenza, Università La Sapienza, direttore: prof. Vittorio Frosini; il Centro Interdipartimentale di ricerca in filosofia del diritto e informatica giuridica, Università di Bologna, Facoltà di Giurisprudenza, direttore: prof. Enrico Pattaro. Questi due enti di ricerca e didattica hanno svolto un ruolo molto significativo per lo sviluppo degli studi, delle ricerche, della didattica in Informatica Giuridica e in Diritto dell'Informatica. E' necessario oggi effettuare un nuovo censimento per verificare la diffusione delle discipline dell'informatica giuridica e del diritto dell'informatica, per comprendere se vi è stata una maggiore diffusione e dove; se ci sono professori di ruolo e ricercatori delle due discipline; se non vi è stata una maggiore diffusione, comprendere i motivi a fronte di una società che da 30 anni si caratterizza come società dell'informazione (a partire dal documento Bangemann del 1994) e dello sviluppo di internet, dei mercati e dei servizi di informazione fino ai social networks (come spesso succede nelle scienze giuridiche oggi il diritto "rincorre" i fenomeni sociali e la "scienza giuridica" non provvede al proprio interno a "rinnovarsi" con nuovi approcci, metodologie, discipline).

3.Il Convegno di Camerino sull'Insegnamento della Informatica Giuridica (1988)

Gli atti del Convegno dell'11 e 12 novembre 1988 sono stati pubblicati nel volume *L'insegnamento dell'informatica giuridica* (Editore Liguori 1990) a cura di Vittorio Frosini e Donato A. Limone. Il Convegno fu organizzato dall'Associazione ANDIG e dalla cattedra di Informatica Giuridica

(Donato A. Limone) con lo scopo di definire alcune linee guida: come fare didattica per e nella l'Informatica giuridica; perché si tratta di una nuova didattica in ragione di questo nuovo ambito disciplinare; perché i corsi di laurea in Giurisprudenza devono comprendere una disciplina come l'Informatica giuridica. L'insegnamento della informatica giuridica per la prima volta era oggetto di un convegno. Nel 1989 a Camerino viene realizzata la prima aula didattica per le ricerche e la didattica del diritto in una Facoltà di Giurisprudenza in Italia con 8 stazioni di lavoro in rete. Dal 1989 la cattedra di Informatica giuridica di Camerino realizza il corso di formazione introduttivo alla tesi di laurea in Giurisprudenza, utilizzando le tecnologie dell'informazione e l'utilizzo delle banche dati giuridici (con la partecipazione di studenti da tutte le parti d'Italia).

4. Metodologia dell'insegnamento del diritto con sussidi tecnologici: il convegno di Roma del 1991.

Gli atti del Convegno di Roma sono stati pubblicati nel 1993 nel volume *Didattica giuridica e informatica*, Milano, Giuffrè, curato da Gianfranco Caridi. Il convegno si è tenuto il 12 dicembre 1991 presso l'Istituto di Teoria dell'Interpretazione e di Informatica Giuridica della Università La Sapienza, organizzato dallo stesso Istituto e dall'ANDIG. Il volume raccoglie le relazioni di Vittorio Frosini, Guido Alpa, Renato Borruso, Gianfranco Caridi, Paolo Galdieri, Donato A. Limone.

5. I corsi di perfezionamento e di master attivati con il supporto dell'ANDIG. Il contesto universitario.

Nel 1988 viene istituito il corso di perfezionamento in informatica giuridica presso la Facoltà di Giurisprudenza dell'Università degli Studi La Sapienza; nel 1998 si registra l'attivazione del corso di perfezionamento in diritto dell'informatica (Università di Lecce); nel 2001 sono attivati i primi Master universitari in diritto dell'informatica delle Università di Lecce, di LUMSA e di Bologna. Il contesto universitario, nel quale operano i docenti di informatica giuridica e diritto dell'informatica, negli anni '90 fa registrare la determinazione dei settori scientifico-disciplinari del 1997 con l'inserimento del diritto dell'informatica nei raggruppamenti disciplinari N01X (diritto privato) e N09X (istituzioni di diritto pubblico); viene confermata la informatica giuridica nel raggruppamento N20X (Filosofia del diritto). Con la rideterminazione dei settori disciplinari del 1999, il diritto dell'informatica è confermato nei raggruppamenti N01X (Diritto privato) e N09X (Istituzioni di diritto pubblico) e l'informatica giuridica è confermata nel settore N20X (Filosofia del diritto). Con la rideterminazione del 4 ottobre 2000 le discipline in questione sono presenti nell'ambito di IUS/20 (Filosofia del diritto), la informatica giuridica; nell'ambito di IUS/01 (Diritto privato) è presente il diritto dell'informatica. Un riconoscimento importante dell'informatica giuridica viene assegnato dal decreto 21 dicembre 1999 n. 537 (Scuole di specializzazione per le

professioni legali). Nell'allegato 1 al decreto si rileva che l'informatica giuridica è materia dell'area A (I° anno).

6. L'Informatica giuridica oggi: il convegno ANDIG di Roma del 1.12.2005.

Al convegno del 2005 l'Andig vi giunge dopo due perdite di due soci fondatori: Vittorio Frosini (Presidente di ANDIG dalla fondazione (1988) al 2001, anno della sua scomparsa) ed Ettore Giannantonio (docente di informatica giuridica e diritto dell'informatica presso la LUISS, socio fondatore Andig, scomparso il 2002). Due figure importanti di studiosi e di uomini. Nel 2002 il Direttore dell'Istituto del CNR "Istituto di Teoria e tecniche dell'Informazione Giuridica", prof. Nicola Palazzolo, presenta al Presidente del CUN la richiesta di costituzione di un nuovo settore scientifico-disciplinare IUS/22 "Diritto e tecnologie dell'informazione", richiesta maturata nell'ambito degli incontri e delle assemblee ANDIG. Nel 2003 chi scrive, nella qualità di Presidente ANDIG, scrive al CUN chiedendo una audizione in merito alla attivazione del nuovo settore scientifico-disciplinare definito IUS/22 "Diritto e tecnologie dell'informazione". La richiesta non fu presa in considerazione.

Nel 1.12.2005 ANDIG organizza il convegno "*L'informatica giuridica oggi*" presso la Facoltà di Giurisprudenza, Università degli Studi di Roma La Sapienza. Il programma prevedeva gli interventi del prof. Carlo Angelici (Preside della Facoltà di Giurisprudenza), del presidente dell'ANDIG (Donato A. Limone), del Ministro per l'Istruzione, l'Università e la Ricerca, Letizia Moratti; del Ministro per l'Innovazione e le tecnologie, Lucio Stanca; del presidente della Società Italiana di Filosofia del diritto, prof. Enrico Pattaro; con la introduzione del prof. Renato Borruso; gli interventi dei professori Giancarlo Taddei Elmi, Leonardo Bugiolacchi, Angela Viola, Giovanni Sartor, Francesco Romeo, Nicola Palazzolo, Costantino Ciampi, Cesare Maioli, Luigi Di Viggiano, Gianluigi Ciacci, Paolo Galdieri.

Gli atti del convegno sono stati pubblicati a cura dell' ITTG nel 2007 con prefazione di Nicola Palazzolo.

7. L'insegnamento del diritto nelle università telematiche.

Con la istituzione delle università telematiche, previste dalla Finanziaria del 2002 e rese operative un Decreto interministeriale del 2003, di sviluppano i corsi di laurea in rete nelle materie giuridiche (così come già auspicato dall'Andig nel 1988). In particolare, l'Università telematica Telma attiva da subito un insegnamento di informatica giuridica (2005) con un professore ordinario della disciplina. E nel 2007 viene attivato dalla stessa università e su iniziativa del Preside della Facoltà di giurisprudenza di tale università (prof. Donato Limone), l'insegnamento di *Scienza dell'amministrazione digitale* (per la prima volta in Italia; ancora oggi non esistono insegnamenti simili in altre università telematiche e non). L'insegnamento (prof. Donato Limone) ha lo scopo

di supportare la fondazione e lo sviluppo dell'amministrazione digitale e di "rifondare" la scienza dell'amministrazione che oggi "inevitabilmente" non può che operare con un nuovo approccio metodologico e di modellistica organizzativa totalmente caratterizzato dal "digitale" (nuovi contesti organizzativi; servizi per i cittadini in rete; semplificazione dell'azione amministrativa; procedimenti amministrativi informatici; gestione digitale del sistema documentale pubblico; forti riduzioni di oneri amministrativi interni e per l'utenza; applicazione del Codice dell'Amministrazione Digitale; formazione rinnovata della dirigenza e dei dipendenti pubblici rispetto al nuovo modello dell'amministrazione digitale; nuovi profili professionali per questa nuova amministrazione).

8. Il nuovo statuto ANDIG del 2012: la rinascita.

Dal 2005 al 2012 si registra un periodo di blocco dell'attività dell'Associazione. Su iniziativa del Presidente della stessa Associazione (Donato A. Limone) i soci interessati decidono di riformare l'ANDIG ed il nuovo statuto viene approvato in data 9.11.2012.

L'Associazione Nazionale Docenti di Informatica Giuridica e diritto dell'informatica (ANDIG) ha come scopo quello di promuovere e svolgere tutte quelle azioni di tipo istituzionale, legislativo, culturale, scientifico e tecnico per la introduzione e lo sviluppo dell'informatica giuridica e del diritto dell'informatica nell'insegnamento, nella ricerca e nella formazione, considerando, in particolare, il contesto della società dell'informazione e della conoscenza e le applicazioni delle tecnologie dell'informazione e della comunicazione.

Per il conseguimento dei propri fini l'Associazione potrà:

- a) promuovere ed avviare tutte le iniziative di tipo normativo ed amministrativo nell'ambito di attività nazionali, comunitarie ed internazionali con lo scopo di creare le condizioni ottimali per un assetto adeguato dell'insegnamento dell'informatica giuridica e del diritto dell'informatica nel sistema dell'istruzione universitaria, post universitario e professionale;
- b) promuovere ed istituire rapporti con Università, Enti, Istituzioni ed Associazioni, sia nazionali sia comunitari ed internazionali, che operano per gli stessi fini dell'Associazione;
- c) istituire rapporti e promuovere iniziative con il mondo delle imprese e con le Pubbliche Amministrazioni per lo sviluppo dei mercati dell'informazione e della comunicazione elettronica e per l'attuazione dell'amministrazione digitale;
- d) promuovere e svolgere studi, ricerche, indagini, progetti;
- e) organizzare convegni, conferenze, seminari;
- f) curare corsi di formazione ed aggiornamento;
- g) curare l'edizione, in modalità analogica e digitale, di pubblicazioni, di documentazioni e materiale didattico.

Possono essere associati dell'Associazione tutti coloro che hanno svolto attività didattica e di ricerca nel campo dell'informatica giuridica e del diritto dell'informatica con riferimento al vigente ordinamento universitario o che sono in possesso di un titolo di master universitario in informatica giuridica, in diritto dell'informatica, in management pubblico ed e-government.

Possono essere altresì associati tutti coloro che operano nel settore delle tecnologie

dell'informazione e della comunicazione nella qualità di funzionari pubblici, di professionisti, di tecnici, di imprenditori.

La rinascita di ANDIG quindi si basa su tre aspetti fondamentali:

- a) informatica giuridica e diritto dell'informatica sono due modi specifici e diversi di considerare il rapporto tra diritto e tecnologie dell'informazione; entrambi concorrono alla definizione di questo rapporto, con approcci diversi sotto il profilo scientifico e metodologico;
- b) apertura dell'Associazione a soggetti che non siano solo docenti delle due discipline ma che si occupino delle tecnologie dell'informazione come operatori, sia privati che pubblici;
- c) la rinascita è strettamente correlata allo sviluppo della Società dell'informazione, e delle relative politiche comunitarie e nazionali, ed al contesto internazionale.

L'Associazione oggi è strutturata in sezioni territoriali ed in gruppi di lavoro:

a) Le sezioni territoriali:

Sezione territoriale Emilia Romagna: sede di Bologna, coordinatore: Prof.ssa Monica Palmirani

Sezione territoriale Toscana: sede di Firenze, coordinatore: prof. Costantino Ciampi

Sezione territoriale Lazio: sede di Roma, coordinatore: prof. Gianluigi Ciacci

Sezione territoriale Puglia, sede di Lecce, coordinatore: Prof. Marco Mancarella

Sezione territoriale Liguria: sede di Genova, coordinatore: prof. Pasquale Costanzo

Sezione territoriale Calabria: sede di Catanzaro, coordinatore: prof.ssa Wanda D'Avanzo

Sezione territoriale Abruzzo, coordinatori: prof.ssa Paola Di Salvatore e prof. Sandro Di Minco

Sezione territoriale Sardegna: coordinatore, prof. Massimo Farina

b) Gruppi di lavoro:

Gruppo di lavoro "Filosofia del diritto e società dell'informazione", coordinatore: Francesco Riccobono, Università Federico II di Napoli

Gruppo di lavoro "Sistemi legislativi digitali", coordinatore, prof.ssa Irene Sigismondi, Unitelma Sapienza

Gruppo di lavoro "Giustizia digitale", coordinatore: prof. Giuseppe Corasaniti, Università di Roma Sapienza

Gruppo di lavoro "Diritto amministrativo e amministrazione digitale" coordinatori: prof. Donato A. Limone, Unitelma Sapienza; prof. Luigi Diviggiano, università del Salento; prof. Marco Mancarella, università del Salento

Gruppo di lavoro "Didattica e ricerca su Informatica Giuridica e Diritto dell'informatica", coordinatore: prof. Giovanni Sartor, Università di Bologna

Gruppo di lavoro "Comunicazione elettronica", coordinatore: prof. Alfonso Contaldo, Unitelma Sapienza

Gruppo di lavoro "Commercio elettronico", coordinatore: prof. Leonardo Bugiolacchi, Unitelma Sapienza

Gruppo di lavoro "Diritto civile dell'informatica", coordinatore: prof. Gianluigi Ciacci, Università Luiss, e Angela Viola, Università Sapienza

Gruppo di lavoro "Diritto penale dell'informatica", coordinatore: prof. Paolo Galdieri, Università Luiss

Gruppo di lavoro "Democrazia elettronica", coordinatore: prof. Pasquale Costanzo, Università di Genova.

9. Il convegno di Roma del 29 ottobre 2013 “I nuovi scenari della società dell’informazione: aspetti politici, giuridici, amministrativi e tecnici”.

Il Convegno viene deciso dal Consiglio direttivo dell’ANDIG, su proposta del Presidente, per “rilanciare” l’Associazione definendo da subito di volere operare (come indicato nel nuovo statuto) con riferimento agli “scenari” della società dell’informazione. Il Convegno viene organizzato da ANDIG e dalla Università telematica Unitelma Sapienza, con il patrocinio di SIIG (Società Italiana di Informatica Giuridica), di ANORC (Associazione Nazionale Operatori e Responsabili della Conservazione digitale), del Laboratorio di eGovernment (LEG) dell’Università del Salento. Il Convegno si è svolto con un programma strutturato in due sessioni con una introduzione del presidente dell’ANDIG, prof. Donato Limone. Le sessioni sono state coordinate dai professori Giovanni Sartor (Università di Bologna) e Francesco Riccobono (Università Federico II, Napoli). Le relazioni hanno trattato temi di attualità della società contemporanea. Gli atti del convegno sono pubblicati in questo volume della Rivista in modalità multimediale (testi scritti e registrazione audio-video degli interventi).

I NUOVI SCENARI DELLA SOCIETÀ DELL'INFORMAZIONE: ASPETTI POLITICI, GIURIDICI, AMMINISTRATIVI E TECNICI APERTURA DEI LAVORI

Multimedia

Intervengono:

- **Prof. Francesco Avallone**, *Rettore di Unitelma Sapienza.*
- **Donato A. Limone**, *Presidente ANDIG, Ordinario di Informatica Giuridica, Unitelma Sapienza.*
- **Francesco Riccobono**, *Prof. Ordinario di Filosofia del Diritto - Università Federico II di Napoli*



Clicca sull'immagine o fotografa il QrCode
per accedere al MediaBook CLIOedu

LA CONVENZIONE SUL CYBERCRIME COME BASE DEL SISTEMA REGOLATORIO UNIVERSALE PER IL CYBERSPAZIO

Giuseppe Corasaniti

 *Multimedia*



Clicca sull'immagine o fotografa il QrCode
per accedere al MediaBook CLIOedu

La Convenzione sul *cyber crime* del 23 novembre 2001¹ non rappresenta il punto di partenza ma il punto di arrivo di un percorso normativo articolato, nato in Europa e definito in Europa, cui gli Stati Uniti hanno subito aderito (insieme al Giappone)². La Convenzione rappresenta, perciò più che un astratto strumentario giudiziario, un vero e proprio *corpus* di regole uniformi e valide sul piano transnazionale e condivise (vi aderiscono ben 41 Paesi) nei cui principi generali si rinvencono comuni precetti destinati ad operare quali prime regole internazionali dell'informatica, definendo condotte e responsabilità, e, soprattutto, consentendo la previsione di strutture operative comuni volte al contrasto effettivo alla criminalità informatica che finora si era giovata di un ambiente "virtuale" di sostanziale impunità ed invisibilità, costituendo forse il più problematico ostacolo allo sviluppo economico globale.

Da una prima fase di regolamentazione molto generale (che in linea di massima si suole individuare dal 1989, data delle prime raccomandazioni in tema di criminalità informatica elaborate proprio dal Consiglio d'Europa) l'attenzione si è gradualmente poi spostata dall'"oggetto" delle attività informatiche, ed in particolare dai dati, qualificati come vere e proprie nuove forme di beni economicamente e socialmente, e quindi giuridicamente rilevanti, fino alla considerazione dell'attività elaborativa informatica vista nel suo insieme in modo organizzato ed articolato, definendone prima le responsabilità sociali, e quindi progressivamente, considerandone i rischi e prefigurando precise responsabilità anche di ordine penale. Solo con la fine del secolo scorso, con l'avvento del *world wide web*, la criminalità informatica viene ad esser progressivamente considerata, sia in ambito interno (solitamente aggiornando l'elenco dei reati contro il patrimonio o la riservatezza individuale) che, soprattutto, in ambito internazionale dal momento che quasi tutte le tecniche criminali hanno fatto leva sulla contemporanea disponibilità di applicazioni gratuite potenzialmente idonee a facilitare le attività criminose come sulla estrema facilità di compiere reati (frodi informatiche o accessi illeciti in particolare) al di fuori dell'ambito territoriale statale ovvero di conseguire il profitto o nascondere informazioni nel medesimo contesto, talora giovandosi di servizi offerti in modo globalizzato ed universale. Era mancato, fino al 2001, uno strumento normativo preciso, e tale mancanza non poteva essere supportata solo dal complesso sistema convenzionale universale : alle difficoltà derivanti da un approccio estremamente burocratico, quale quello definito nei classici trattati di mutua assistenza internazionale bilaterale sia aggiungeva la difficoltà di esperire tutte le formalità in tempi assai ristretti, di acquisire validi riscontri o elementi di prova in modo preciso, e soprattutto di non poter disporre di alcun sistema integrato e rapido di mutua assistenza.

Ed infatti, richiamando i compiti istituzionali del Consiglio d'Europa la Convenzione è espressamente considerata quale strumento sia per realizzare un'unione più stretta tra i suoi membri che per promuovere tra di essi il *valore della cooperazione internazionale*, riconoscendo la necessità di perseguire, in via prioritaria, *una politica penale comune finalizzata alla protezione della società*

¹ <http://www.conventions.coe.int/Treaty/en/Treaties/Html/185.htm>

² D'altronde già i primi commenti intuirono la portata autenticamente innovativa della Convenzione. Cfr. AMORE S. *Quei reati on line: criminali nelle rete. Strasburgo lancia il manuale di difesa. Dalla Convenzione le armi contro pedopornografia e terrorismo*, in *Diritto e giustizia* 2006 pag. 91, MANZIONE D. *Consiglio d'Europa e cybercrime* in. *Legislazione penale* 2005 pag. 305, MUSACCHIO V. *Criminalità organizzata e cybercrime*, *Diritto e diritti* 2003 pag. 2. MAGGIPINTO A., *Reati nella Rete, tutti i nodi da sciogliere. Se il cybercrime mette in crisi il Codice*, in *Diritto e giustizia* 2006 pag. 61.

contro la criminalità informatica, tra l'altro, attraverso l'adozione di una legislazione interna appropriata e per favorire la conseguente cooperazione internazionale. Tra le premesse, in primo luogo, viene considerata la nuova fase dell'era digitale ed i profondi cambiamenti introdotti dalla *digitalizzazione, convergenza e continua globalizzazione delle reti informatiche*. Ciò ha posto, di conseguenza, il problema prioritario di evitare il rischio che le reti informatiche e le informazioni elettroniche possano essere utilizzate sistematicamente per commettere reati rendendo così possibile che le prove relative a tali reati possano essere a loro volta memorizzate e trasferite e, soprattutto, rese disponibili in funzione dell'esercizio dell'azione penale. Gli stati promotori, riconoscono, infatti, come centrale la *necessità di cooperazione tra pubblico e privato nella lotta contro la criminalità informatica* e la necessità di *tutelare l'uso e lo sviluppo delle tecnologie dell'informazione*.

Di conseguenza si sottolinea come una lotta efficace contro la criminalità informatica richieda una rapida e ben funzionante cooperazione internazionale in materia penale, infatti la Convenzione viene intesa anche come strumento essenziale per scoraggiare *l'azione criminale diretta contro la riservatezza, l'integrità e la disponibilità dei sistemi informatici, delle reti e dati informatici*, nonché l'uso improprio di tali sistemi, reti e dati, fornendo per la criminalizzazione di tale condotta, disposizioni penali comuni ed favorendo la adozione di servizi istituzionali per combattere efficacemente tali reati, facilitandone la individuazione, e le relative indagini e azioni penale sia a livello nazionale che internazionale e prevedendo quindi forme di cooperazione internazionale particolarmente veloci e affidabili.

Ed è proprio la premessa a evidenziare come la Convenzione sia da considerare parte di un più complesso ed articolato equilibrio tra gli interessi delle necessarie misure di carattere legislativo di contrasto di legge ai reati informatici e rispetto dei diritti umani fondamentali sanciti sin dal 1950 dalla Convenzione del Consiglio d'Europa per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e dal Patto internazionale delle Nazioni Unite sui diritti civili e politici di diritti e altri trattati internazionali applicabili sui diritti umani. Si sottolinea preliminarmente, infatti, in particolare il diritto di ognuno di avere opinioni senza interferenze, così come il diritto alla libertà di espressione, *compresa la libertà di cercare, ricevere e diffondere informazioni e idee di ogni specie, indipendentemente dalle frontiere*, garantendo però i diritti fondamentali relativi al rispetto della vita privata. Ed ancora viene richiamata espressamente proprio la Convenzione del Consiglio d'Europa del 1981 sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale e la Convenzione del 1989 delle Nazioni Unite sui diritti del fanciullo. Due richiami, questi, che saranno essenziali per cogliere lo sviluppo articolato delle norme internazionali, da un lato, infatti si riconosce la priorità di una azione penale attenta ai diritti fondamentali sul *web*, e dall'altro si manifesta per la prima volta attenzione ai soggetti più deboli, in particolare ai minori³, per cui l'accesso alle informazioni globalizzate costituisce occasione di crescita culturale, ma anche il rischio per l'accesso a contenuti in grado di pregiudicarne la libera formazione senza adeguata mediazione. Ed infatti in tale prospettiva si riconosce come la Convenzione costituisca

³ E in questo senso appare fondamentale anche la più recente Convenzione di Lanzarote del 2007 (ratificata in Italia con la legge 1-1-2012 n. 127, a sua volta integrativa di numerose ipotesi di reato che l'Italia aveva già previsto sin dalla Legge 3 agosto 1998, n. 269 n. in merito cfr. ALBAMONTE E. e MONTELEONE M. *Ratifica ed esecuzione della Convenzione di Lanzarote*. Giur. merito 2013 pag. 752 e 1484 (rispettivamente a commento delle modifiche introdotte alle disposizioni penali e processuali penali), MARI A. *Le principali novità introdotte dalla legge attuativa della Convenzione di Lanzarote*, Cass. Pen. 2012 pag. 3956.

elemento integrativo essenziale delle convenzioni del Consiglio d'Europa sulla cooperazione nel settore penale, così come i trattati già esistenti tra il Consiglio degli Stati membri Europa e in altri Stati ⁴, ponendosi espressamente come strumento normativo innovativo ed organico al fine di effettuare indagini nei procedimenti penali relativi a reati connessi ai sistemi informatici e ai dati più efficaci e per consentire la raccolta di prove in formato elettronico di un reato, pervenendo alla costituzione di vero e proprio un *sistema rapido ed efficace di cooperazione* internazionale funzionale alle esigenze specifiche della lotta contro la criminalità informatica.

Il nucleo tematico essenziale della Convenzione finisce, così, per preconstituire una *serie comune e correlata di definizioni* destinate a porsi come comuni nel suo ambito applicativo pressoché globale. E non si tratta di un aspetto secondario, se è vero che proprio sul terreno definitorio, cioè proprio sulla esigenza di predisposizione di un quadro di riferimento “tecnico” univocamente condiviso, che potevano esser rinvenute le principali difficoltà di una regolamentazione internazionale coerente ed uniforme. ⁵. Sotto tale aspetto la Convenzione richiama alcune definizioni di ordine generale (peraltro in larga parte ispirate dalla regolamentazione dell'Unione Europea in materia di servizi elettronici nelle telecomunicazioni) concentrandosi, nella definizione delle condotte criminose più sulla specifica individuazione dei *beni giuridici*⁶ da garantire in un ambito di condotte oggettivamente riconoscibili in quanto tali, lasciando poi ai singoli Stati aderenti la possibilità di incidere più o meno marcatamente sull'elemento soggettivo dei singoli reati, sia in relazione all'intensità del dolo che, soprattutto, in ragione degli effetti concreti della singola condotta. Il quadro normativo appare perciò estremamente delicato ed in un certo senso reso più complesso dalla interazione tra elementi definitori solo apparentemente penalistici e considerazione analitica della condotta “*informatica*” vista nel suo insieme e nella sua essenza intrinsecamente “globale”.

Ne consegue che l'analisi del testo della Convenzione non può forse limitarsi ai soli, pur importanti, aspetti penalistici (elementi soggettivi ed oggettivi dei reati ivi previsti) ma deve forse spingersi in termini molto più aperti, fino a considerare la novità di un trattato internazionale che per la prima volta tenta di individuare strumenti definitivi ed operativi comuni su un territorio “virtuale” quale il *cyberspazio*, l'intreccio metaforico delle connessioni telematiche che può annullare ogni concetto genericamente riferito al limite territoriale o spaziale di competenza statale e che perciò pretende metodi di approccio alla problematica molto più aperti ed effettivamente innovativi, se si pensa che, a differenza della maggior parte dei trattati internazionali viene per la prima ad essere definito un “ambito” spaziale di comune interesse, entro il quale gli Stati possono -individualmente e in cooperazione- intervenire più sfumatamente in modo regolatorio, ma soprattutto “devono” intervenire per garantire con gli strumenti del diritto penale comune, la libera fruizione di beni giuridici ormai essenziali alla convivenza civile, sociale ed economica⁷.

⁴ Sulla rilevanza diretta ormai delle dichiarazioni di garanzia dei diritti nella costruzione dello spazio penale europeo cfr. ANDOLINA E. *Nuovi scenari nella tutela penale dei diritti fondamentali in Europa*. Dir. penale e processo 2012 pag. 764, ZERMAN M.P. *Europa: il sistema integrato di tutela dei diritti fondamentali*. Rass. Avv. Stato 2011 pag. 44.

⁵ Cfr. infatti COLOMBO E. *La cooperazione internazionale nella prevenzione e lotta alla criminalità informatica: dalla Convenzione di Budapest alle disposizioni nazionali*, CIBERSPAZIO E DIRITTO 2009 pag. 285, FULVI F.R. *La Convenzione sul Cybercrime e l'unificazione del diritto penale dell'informatica*, in Diritto penale e processo 2009, pag. 639.

⁶ Ed appare evidente la rilevanza sotto il profilo del bene giuridico, rinviandosi ai fondamentali studi di BRICOLA F., *Teoria generale del reato*, Novissimo Digesto 1973, pag.86.

⁷ Ed è bene in modo particolare riflettere sulle esigenze di sistematicità nell'approccio regolatorio alle tecnologie

All'art.1 sono contenute le definizioni, che costituiscono quindi un riferimento interpretativo comune ed uniforme, viene adottata una definizione unitaria di “*sistema informatico*” e cioè qualsiasi dispositivo o gruppo di dispositivi interconnessi o collegati, uno o più dei quali, secondo un programma, svolge un trattamento automatico di dati. Analogamente viene adottata una nozione uniforme di “*dati informatici*” e cioè qualsiasi rappresentazione di fatti, informazioni o concetti in una forma idonea alla trasformazione in un sistema informatico, compreso un programma che svolga una specifica funzione nel sistema.

Nuova, ed in un certo senso più elastica appare anche la definizione di “*prestatore di servizi*”, che ricomprende qualsiasi soggetto pubblico o privato che *fornisce agli utenti del suo servizio la capacità di comunicare per mezzo di un sistema informatico o qualunque altro soggetto che elabora e memorizza i dati informatici per conto di tale servizio di comunicazione o agli utenti di tale servizio*. Infine sono considerati i “*dati relativi al traffico*” e cioè i dati informatici relativi a una comunicazione per mezzo di un sistema informatico, generato da un sistema di computer ove si è formata una parte della catena di comunicazione (compresi l'origine della comunicazione, destinazione, itinerario, ora, data, dimensione, durata, o il tipo di servizio sottostante).

Sono quindi specificamente enucleati i reati “comuni” di carattere informatico (i c.d. “reati informatici in senso stretto”), in una sezione che è espressamente qualificata di “diritto penale sostanziale”. Si tratta di reati accomunabili dal bene giuridico tutelato della “*riservatezza, integrità e disponibilità di dati e sistemi informatici*”⁸. Ne consegue una comune definizione di “*accesso illecito*” (art.2) come di “*intercettazione illegale di comunicazioni informatiche*” (art.3) e di *danneggiamento informatico* di dati (art.4), di “*interferenza illecita*” (art.5) così come di abuso (cioè per fini programmati di danneggiamento o di sistematica commissione di reati) di dispositivi informatici, incluso il software (art.6). Così viene dettata una descrizione univoca del reato di *falso informatico* (art.7) con riferimento ai dati ed alle falsificazioni di carattere digitale e delle frodi informatiche (art. 8) definite in relazione al danno patrimoniale, commesso intenzionalmente mediante abusiva utilizzazione, alterazione, cancellazione o soppressione di dati informatici e qualsiasi interferenza con il funzionamento di un sistema informatico *svolta con intento fraudolento a fini di profitto*⁹.

Il Titolo 3 della Convenzione si occupa, quindi dei *contenuti elaborati attraverso sistemi informatici* e definisce in primo luogo (art.9) i reati in materia di pedo pornografia comprendendo in tale condotta ogni contenuto riferito a un minore coinvolto in condotte sessualmente esplicite, ovvero una persona solo somigliante a un minore coinvolto in condotte sessualmente esplicite ovvero immagini realistiche che rappresentano un minore coinvolto in una condotta sessualmente esplicita.

per la prima volta, magistralmente, individuate da Vittorio FROSINI, in *I giuristi e la società dell'informazione, Diritto dell'informazione e dell'informatica 1996 pag. 17.*

⁸ Peraltro la stessa problematicità dell'oggetto dei reati informatici in quanto intrinsecamente rivolti a oggetti giuridici di carattere omologo era stata autorevolmente prospettata da GIANNANTONIO E. *L'oggetto giuridico dei reati informatici* Cass.pen.2001,pag. 2244. Successivamente lo stesso A. nel fondamentale saggio *I reati informatici, Diritto dell'informazione e dell'informatica 1992 pag. 335* si era sforzato per evidenziare gli elementi comuni unificanti i c.d. “reati informatici in senso stretto” (cioè commessi esclusivamente ed unicamente attraverso il computer) analizzando le differenti modalità di incisione sui beni giuridici di carattere tradizionale. L'analisi di GIANNANTONIO in Italia è forse la prima a muoversi sul terreno dell'oggetto giuridico del reato, senza disperdersi nell'ambito di una pura e formale disamina di carattere penalistico.

⁹ Cfr. PICOTTI L. *La nozione di “criminalità informatica” e la sua rilevanza per le competenze penali europee. Riv. Trim. diritto penale ed economia 2011 pag. 827.*

Sono parimenti sanzionabili sia le condotte di carattere produttivo o riproduttivo che quelle di carattere distributivo mediante sistemi informatici ed anche il semplice possesso di contenuti in un sistema informatico o su un supporto di memorizzazione di dati informatici.

Analogamente la Convenzione (art.10) considera le ipotesi di violazione della proprietà intellettuale sottolineando peraltro la diretta connessione con la Convenzione di Berna e la stretta attenzione agli aspetti soggettivi della condotta svolta attraverso un sistema informatico, secondo modalità ben precise ed univocamente prospettate (volontariamente, su scala commerciale e per mezzo di un sistema informatico). Sul piano più generale è sempre la Convenzione (art.11) a determinante anche le ipotesi di responsabilità c.d. “accessorie” nei reati informatici, quali *il tentativo o il concorso* (art.11) ovvero le ipotesi, articolate, di *responsabilità delle persone giuridiche* (art.12)¹⁰ nei casi in cui la carenza di vigilanza o di controllo abbia reso possibile il reato, in modo autonomo rispetto alla responsabilità di ordine penale e civile. A riguardo sono prescritte sanzioni (art.13) *purché effettive, proporzionate e dissuasive*. Appare evidente anche che la lettura della Convenzione rafforza proprio nella previsione di una responsabilità delle persone giuridiche un fondamentale sostegno alle vittime dei comportamenti illeciti e non prevede alcuna limitazione nell’ambito dei reati (informatici) presupposti, sicché tale forma di responsabilità appare integrale e diretta, e soprattutto imposta a livello interno dalla disciplina internazionale.

La sezione 2 della Convenzione è formalmente dedicata agli aspetti di “*diritto processuale (penale)*” ed impone agli Stati aderenti (art.14) di adottare le misure legislative e di altra natura che dovessero essere necessarie per definire i poteri e le procedure di specifiche indagini o procedimenti in relazione a uno dei reati stabiliti dalla convenzione ma, altresì, agli altri reati commessi mediante un sistema informatico, o la raccolta di prove in formato elettronico (digitale) di un reato. Sotto questo profilo assume una rilevanza centrale l’art. 15 (*condizioni e garanzie*) che finisce per coniugare indissolubilmente il nuovo sistema di procedure e di comunicazioni in materia di *cybercrime* con le garanzie, anche eventualmente già poste a livello nazionale, dei diritti umani e delle libertà, compresi i diritti derivanti ai sensi obblighi assunti nell’ambito della Convenzione del 1950 del Consiglio d’Europa per la salvaguardia dei diritti dell’uomo e delle libertà fondamentali, e del Patto internazionale delle Nazioni Unite sui diritti civili e politici del 1966 nonché ad altri strumenti internazionali eventualmente applicabili in materia di diritti umani, nel fondamentale rispetto del *principio di proporzionalità*.

Ed è fondamentale, peraltro, che tra le condizioni e garanzie essenziali siano ricomprese tanto la *supervisione giudiziaria* in generale sulla sua applicazione, sia possibili limitazioni di carattere statale del campo di applicazione o di durata di funzioni o procedure richiamanti le disposizioni internazionali. Si sottolinea in modo particolare come nel rispetto del principio fondamentale di coerenza con l’interesse pubblico, ed in particolare con l’interesse pubblico alla buona amministrazione della giustizia, ciascuna parte dovrebbe sempre (prioritariamente) considerare l’impatto dei poteri e delle procedure sui diritti, le responsabilità e gli interessi legittimi di terzi. Si tratta di una importante sottolineatura, che evidenzia come, al di là della specifica esigenza acquisitiva deve essere sempre e comunque assicurato un costante ed effettivo equilibrio nella adozione di tecniche meno invasive e più mirate, e nella preparazione culturale della magistratura e delle forze di polizia che non potrà

¹⁰ Cfr. in particolare RUGGIERI F., “*Cybercrime*” e *responsabilità amministrativa degli enti* in *Diritto e pratica delle società* 2008 pag. 6.

che manifestarsi mediante una ampia e comune sensibilizzazione culturale.

E' significativo che proprio tale circostanza e cioè il pregiudiziale rispetto delle convenzioni in tema di diritti fondamentali e delle libertà civili viene espressamente poi richiamata, e persino ripetuta, nell'ambito di ogni singola misura operativa comune prevista, quasi a ribadire perciò la coerenza implicita dell'impianto normativo internazionale, e la sua funzionale tendenza oltre che di strumento investigativo -mai generalizzato, ma precisamente direttamente collegabile in quanto definito in senso "processuale" a diritti e libertà internazionalmente riconoscibili – alla garanzia dei beni giuridici definiti ormai a livello universale e violati, cui le disposizioni non fanno altro che fornire, con l'esercizio dell'azione penale, un supporto essenziale destinato a qualificare ed a rendere efficace l'azione penale, nei diversi ordinamenti coinvolti, e soprattutto per mettere in luce linearmente i rapporti comunicativi digitali nella loro integralità ¹¹, consentendone in modo omogeneo la ricostruzione e la (trasparente) imputabilità a soggetti giuridici ben determinati.

La puntualizzazione appare in sé determinante, in quanto sembra prospettare ancora un duplice profilo problematico : quello della (efficace) attivazione di procedure internazionali volte alla ricerca della prova in termini di supervalutazione degli aspetti autenticamente criminali in ambito internazionale (segnatamente attraverso la funzionale acquisizione dei dati occorrenti all'estero) ovvero in termini specularmente del tutto opposti, volti invece a conseguire piuttosto un effetto "preventivo" mediante acquisizione di dati a carattere massivo per ricostruire successivamente relazioni rilevanti in determinati ambiti spaziali, temporali, economici.

In buona sostanza quello che la Convenzione tratteggia è un punto di equilibrio certo, per la definizione di procedure acquisitive realmente "funzionali" e, soprattutto, (effettivamente) utili alle indagini, tali cioè da potere assicurare la identificazione dei soggetti responsabili e da enucleare con sufficiente grado di precisione e chiarezza le relazioni esistenti eventualmente tra più soggetti coinvolti, ciascuno soggetto potenzialmente a differente giurisdizione.

Nell'ambito delle differenti procedure acquisitive oggi previste internazionalmente solo la considerazione preliminare in ordine alla loro *necessaria utilizzabilità in funzione processuale* (e quindi nei confronti di un accertamento giudiziario già aperto soggetto a precise regole processuali e con le opportune garanzie difensive) finisce per connotare la cooperazione in modo sostanzialmente funzionale al ripristino della legalità in un contesto nel quale ogni accertamento, ed ogni acquisizione informativa, non può che valutarsi se non considerando primaria l'esigenza di ricostruzione, sotto il profilo tecnico e nel complesso ambiente delle relazioni telematiche transnazionali, di azioni e condotte umane precisamente enucleabili, alle quali corrispondono (nei limiti tradizionali posti in chiave ordinamentale) altrettante responsabilità individuali di ordine penale¹².

E quindi vengono definiti gli strumenti operativi comuni, quali *la conservazione rapida di dati informatici* (Articolo 16), mediante apposito ordine acquisitivo di dati informatici *specifici*, compresi i dati di traffico, che siano memorizzati entro un sistema informatico, in particolare quando sussistano motivi per credere che i dati siano soggetti a perdita o modificazione. L'ordine di preservazione

¹¹ Sui profili problematici della "prova digitale" cfr. in particolare MARAFIOTI L. *Digital evidence e processo penale.*, Cass. Pen. 2011 pag. 4509. Per una attenta analisi dei profili problematici della "digital evidence" cfr. MOLINARI F.M. *Le attività investigative inerenti alla prova di natura digitale*, Cass. Pen. 2013 pag. 1259.

¹² E difatti l'art. 14 della Convenzione specifica come l'acquisizione informativa processuale si concepisce "for the purpose of specific criminal investigations or proceedings."

(che prevede un periodo massimo di novanta giorni, eventualmente rinnovabile) comprende anche l'adozione di specifiche misure di custodia e di conservazione nonché di riservatezza sulle procedure. Così è prevista (art.17) la *conservazione rapida e divulgazione parziale dei dati di traffico* anche indipendentemente dal fatto che uno o più fornitori di servizi sono stati coinvolti nella trasmissione di tale comunicazione, per consentire alle autorità interessate di identificare i fornitori di servizi e il percorso attraverso il quale la comunicazione è stata trasmessa. Così viene disciplinato *l'ordine di produzione* (art.18) misura qualificata come “indispensabile” al fine di acquisire da parte delle autorità inquirenti i dati del computer specificati che risultino memorizzati o comunque conservati su supporto, nonché ogni altro dato relativo a servizi offerti on line o informazioni su utenti o abbonati in possesso o sotto il controllo dei fornitori di servizi, compresi numero d'identità del sottoscrittore, indirizzo postale o geografico, telefono e altri tipi di accesso, fatturazione e informazioni di pagamento, disponibili sulla base del contratto di servizio o intesa e ricomprendenti anche aspetti tecnici o di settaggio di eventuali apparati utilizzati. Tra gli strumenti operativi risalta quello di cui all'art. 19 (*perquisizione e sequestro di dati informatici registrati* ¹³ rivolto alla acquisizione diretta della prova in formato digitale, concepita anche in modo sequenziale, onde assicurare l'acquisizione di dati contenuti o memorizzati o comunque accessibili o disponibili su sistemi informatici. Proprio tale disposizione sottolinea la *essenzialità della preservazione tecnica dell'integrità dei dati così acquisiti*, la acquisizione viene ad essere così concepita sia attraverso un accesso diretto al dato interessato nel sistema, sia mediante espressa autorizzazione alle autorità competenti per rimuovere, per accedere ai dati, le protezioni (logiche) eventualmente apposte per inibire l'accesso ai dati stessi. Più complessa appare la *raccolta in tempo reale dei dati di traffico* (Articolo 20) misura che consente la raccolta dei dati (limitata in base alle obiettive capacità tecniche richieste al *provider*) in tempo reale, di comunicazioni specificate trasmesse mediante un sistema informatico. Si tratta, in tutta evidenza, di una misura estremamente ampia, destinata a ricomprendere tanto i dati “esterni” delle comunicazioni che quelli “descrittivi” nel caso di messaggistica (*header destinatario, oggetto, allegati, posizione geografica del mittente o del destinatario*) secondo i protocolli di fatto utilizzati. Ed infine l'art. 21 garantisce la possibilità di *intercettazione di contenuti* di comunicazioni in relazione ad una serie di *gravi reati* determinati dalla legge nazionale, per autorizzare le proprie autorità competenti a raccogliere o registrare contenuti mediante applicazione di strumenti tecnici sul territorio, anche attraverso un vero e proprio obbligo di cooperazione tecnica dei fornitori di servizi.

Il richiamo formale alla “gravità” del reato presupposto finisce, qui, per sottolineare ancora come la misura maggiormente invasiva per le comunicazioni, cioè l'acquisizione diretta dei contenuti, non possa poi che collegarsi alla esigenza (controllata dalle disposizioni processuali penali interne e sottoposta alla supervisione giudiziaria) di riconduzione “coerente” della misura ad effettive e serie violazioni sostanziali del diritto penale interno, di tale intensità e qualificazione in rapporto ai beni giuridici tutelati, da incidere in termini oggettivamente percepibili - in quanto “gravi” e appunto socialmente evidenti, riflessi appunto nella stessa qualificazione formale e quantificazione della sanzione concretamente prospettabile - su interessi individuali o collettivi direttamente

¹³ Per una rassegna problematica, in particolare rivolta alla attuazione italiana della disposizione cfr. MOLINARI F.M. *Questioni in tema di perquisizione e sequestro di materiale informatico*. Cass. pen. 2012 pag. 696 nonché NOVARIO F. *Criminalità informatica e sequestro probatorio: le modifiche introdotte dalla L. 18 marzo 2008, n. 48 al codice di procedura penale*. in Riv. Dir. processuale 2008 pag. 1069.

percepibili e considerati come intrinsecamente prioritari (la persona, la vita, la dignità o la libertà personale, il patrimonio). Alla gravità dell'offesa giuridica corrisponde, perciò, la disponibilità in sede di accertamento internazionale dello strumento più idoneo a rivelare direttamente i contenuti, oltre che le relazioni interpersonali, ma nell'ambito di garanzie ben definite e entro una precisa prospettiva funzionale "processuale", peraltro estremamente variabile dal punto di vista formale nell'ambito dei differenti ordinamenti giuridici interessati, cioè destinata a fornire specifici elementi di riscontro a responsabilità personali di carattere penale già accertate o in via di completo accertamento.

Merita attenzione specifica anche l'art. 22 (*competenza*), che obbliga gli Stati contraenti ad adottare misure necessarie a stabilire (prioritariamente) la competenza in tema di reati informatici ogni qual volta il reato è commesso sul suo territorio, o in luogo equiparato (nave o aeromobile) e da un suo cittadino, se il reato è punibile penalmente in cui è stato commesso o se il reato è commesso al di fuori della giurisdizione territoriale di uno Stato. Tale disposizione sembrerebbe implicitamente richiedere una disciplina processuale specifica delle competenze territoriali giudiziarie in tema di reati informatici, che dovrebbero apparire immediatamente certe, tanto più, appunto in presenza di istanze acquisitive di carattere nazionale. In ogni caso ogni parte adotta misure appropriate in materia di estradizione ed è sempre possibile la riserva di giurisdizione in base al diritto interno, operandosi apposite procedure di consultazione al fine di determinare la giurisdizione in ogni caso di contrasto. La cooperazione internazionale così definita si presenta come "concreta" e, soprattutto "operativa" governata dai principi generali posti dall'art.23 (*Principi generali relativi alla cooperazione internazionale*) per cui gli aderenti cooperano tra loro, in conformità con le disposizioni, e attraverso l'applicazione di strumenti internazionali pertinenti in materia di cooperazione internazionale in materia penale, accordi conclusi sulla base di una legislazione uniforme o di reciprocità, e leggi nazionali, garantiscono in ogni caso la più ampia possibile cooperazione, *ai fini di indagini o procedimenti relativi a reati connessi ai sistemi informatici e ai dati, o per la raccolta di prove in formato elettronico di un reato.*

Si tratta, in buona sostanza, di una cooperazione internazionale autenticamente "digitale" che non è affatto limitata ai soli reati informatici, ma si estende ad ogni profilo acquisitivo di informazioni o dati in ambito digitale che, in linea con gli obiettivi generali della Convenzione e nel rispetto dei suoi principi fondamentali, possa riguardare in ambito penale l'informatica nel suo insieme e quindi qualsiasi comunicazione o registrazione digitale rilevante che possa essere utilizzata nell'ambito di indagini penali, volta a documentare lo stato di un sistema o i dati ivi contenuti, ma anche ad esempio gli interventi ovvero i fatti dei quali nel sistema informatico è rimasta, direttamente o indirettamente, traccia volti a comprovare anche elementi informativi autonomamente rilevanti (il posizionamento territoriale di un utente, le sue comunicazioni, i contenuti cui ha avuto accesso o che sono stati acquisiti) e che possono perciò documentare una condotta ovvero una relazione in termini positivi o negativi.

Ed infine la Convenzione detta norme integrative in tema di estradizione (art.24) e fissa principi generali in tema di *assistenza reciproca* (art.25) che dovrà essere *più ampia possibile*, al fine di indagini o procedimenti relativi a reati connessi ai sistemi informatici e ai dati, o per la raccolta di prove in formato elettronico di un reato e manifestarsi anche con richieste di informazione e mutua assistenza con mezzi di comunicazione, compresi fax o e-mail, nella misura in cui tali mezzi di fornire adeguati livelli di sicurezza e di autenticazione (compreso l'uso della crittografia, se

necessario), con successiva eventuale conferma formale. Possono essere così spontaneamente divulgate informazioni utili alla individuazione degli autori di reati informatici (art.26) sempre in una ottica di assistenza internazionale.

Sono definite procedure relative alle richieste di assistenza reciproca in assenza di accordi internazionali applicabili (art.27) con comunicazione diretta tra gli Stati aderenti mediante le autorità centrali designate ed in caso di urgenza, le richieste di assistenza reciproca o comunicazioni ad esse relative possono essere inviate direttamente dalle autorità giudiziarie della Parte richiedente a tali autorità della Parte richiesta. In questo quadro hanno una funzione essenziale i “punti di contatto” (*Articolo 35 - 24/ 7 Network*) disponibili in ogni Stato aderente 24 ore su 24 , per sette giorni a settimana, al fine di garantire proprio mediante una vigilanza costante e una risposta urgente alle richieste di assistenza (provenienti dall'estero o dirette all'estero) ai fini di indagini o procedimenti relativi a reati connessi ai sistemi informatici e di dati o per la raccolta di prove in formato elettronico di un reato. Tale assistenza include *ogni facilitazione* , o, se consentito dalla sua legge e prassi nazionale, fornitura diretta di prestazioni di consulenza tecnica, conservazione dei dati e raccolta di prove, fornitura di informazioni giuridiche o giudiziarie, e localizzazione nel territorio nazionale dei soggetti indagati.

Il percorso di integrazione e di adattamento della Convenzione alle normative interne si presenta complesso e qualche volta difficoltoso¹⁴ (e l'Italia non sembra certo costituire eccezione, anche se ha il vantaggio di avere anticipato dal 1993 con la legge n. 547 alcune fattispecie penali che prevedevano i reati di accesso illecito, di frode informatica, di danneggiamento informatico, di intercettazioni informatiche adattando le prescrizioni generali dei codici penale e si procedura penale) e la cooperazione internazionale necessita di metodi operativi efficaci e di soggetti istituzionali destinati ad applicarli ben organizzati e soprattutto ben attenti alle diverse implicazioni offerte dall'evolversi delle tecnologie e dalle problematiche di rispetto costante dei diritti fondamentali (dei potenziali indagati così come, soprattutto, delle potenziali vittime dei reati)¹⁵. L'attuazione in Italia della Convenzione è stata affidata alla legge 18 marzo 2008 n. 48 che ha previsto innanzitutto l'adeguamento delle disposizioni del codice penale, del codice di procedura penale e della legge 231/2001 che disciplina la responsabilità degli enti e delle persone giuridiche.¹⁶ Il primo terreno di sviluppo della Convenzione in tema di contenuti digitali è dato, quindi, dal *Protocollo addizionale relativo all'incriminazione di atti di natura razzista e xenofobica commessi a mezzo di sistemi informatici* (2003) allo stato sottoscritto da 20 Paesi. Si tratta di un testo di fondamentale

¹⁴ V. infatti le critiche di CAJANI F. *La Convenzione di Budapest nell'insostenibile salto all'indietro del Legislatore italiano, ovvero: quello che le norme non dicono... Brevi cenni sui problemi di giurisdizione che emergono in tema di intercettazioni telematiche e di data retention e sui correlativi ostacoli all'azione investigativa di contrasto al crimine*. CIBERSPAZIO E DIRITTO 2010 pag. 185. Per una rassegna giurisprudenziale sulla legge 48 cfr. FELCHER I.V. Una rassegna giurisprudenziale con riferimento alla Legge n. 48 del 2008 e alle investigazioni digitali. CIBERSPAZIO E DIRITTO 2013 pag. 131. Per una analisi completa delle disposizioni sostanziali cfr. PICOTTI L. Profili di diritto penale sostanziale della legge n. 48/2008 Dir. penale e processo 2008 pag. 700. Una analisi attenta ai profili più strettamente processuali (che peraltro ricalcano le disposizioni vigenti è quella di LUPARIA L. *I profili processuali della legge 18 marzo 2008 n. 48* in Dir. penale e processo 2008 pag. 717.

¹⁵ RESTA F. *Cybercrime e cooperazione internazionale, nell'ultima legge della legislatura.*, Giur. merito 2008 pag. 2147.

¹⁶ Cfr. in particolare GUERNELLI M. *La legge di ratifica ed esecuzione della Convenzione sul Cybercrime: considerazioni sostanziali e processuali.*, in Riv. Trim. dir. penale ed economia 2008 pag. 753. Per un organico commento della Convenzione sia consentito il rinvio a CORASANITI G. –CORRLAS LUCENTE G. (a cura di) *Cybercrime, responsabilità degli enti, prova digitale*, Padova 2009.

importanza ma certo anche di evidente delicatezza dal punto di vista delle implicazioni politiche, anche perché nell'ambito di tale disciplina viene non solo a essere incriminata la (oggettiva) diffusione di contenuti (audio, video, testi) direttamente incitanti alla discriminazione o all'odio etnico religioso o razziale ma perché contiene per la prima volta una disciplina dei reati di diniego, giustificazione o approvazione di atti di genocidio o dei crimini contro l'umanità (art.6) , con una definizione che si ricollega ad una sorta di riconoscimento implicito del giudicato delle corti penali internazionali¹⁷.

Sul piano pratico non mancano i programmi di addestramento tecnico operativo sviluppati proprio in sede di Consiglio d'Europa, volti a definire in senso più efficace una *strategia uniforme di procedure di carattere tecnico*, attraverso la predisposizione di specifici gruppi di lavoro comuni e di un comune Comitato di attuazione, aperto alle istituzioni europee. E non mancano fondamentali progetti sul piano della estensibilità delle disposizioni della Convenzione anche ai server c.d. "virtuali" come il *cloud computing* onde ottenere comunque elementi informativi utili¹⁸ collegando e scambiando i dati disponibili sulle connessioni¹⁹.

Infine va registrato un significativo tentativo di allargamento del già ampio numero dei Paesi aderenti alla Convenzione, verso l'area dell'Est Europeo (appare imminente l'adesione della Russia) e verso la Cina e l'Africa, prospettandosi così la nascita del primo, autentico atto di regolamentazione giuridica penale universale, considerando che sono ormai 140 i Paesi che hanno adottato specifiche normative sul Cybercrime e che potrebbero ben presto avanzare richiesta di adesione.

Il testo della Convenzione si avvia perciò ad essere la prima, vera, legge universale sul Cyberspazio con una valenza obiettivamente generale, ed una considerazione della cooperazione internazionale che in passato è stata propria solo di trattati aventi più marcatamente contenuti di carattere tecnico, con una graduale e prevedibile progressiva espansione nel prossimo decennio anche del ruolo della Organizzazione delle Nazioni Unite²⁰ in un quadro di armonizzazione e di cooperazione autenticamente universale.

¹⁷ <http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm>

¹⁸ http://www.coe.int/t/dgbl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/TCY_2013_7E_GN3_transborder_V2public.pdf

¹⁹ Cfr. a riguardo TROIANO G. *Profili civili e penali del cloud computing nell'ordinamento giuridico nazionale: alla ricerca di un equilibrio tra diritti dell'utente e doveri del fornitore*. CIBERSPAZIO E DIRITTO 2011 pag. 223.

²⁰ http://www.unodc.org/documents/commissions/CCPCJ_session22/13-80699_Ebook_2013_study_CRP5.pdf

LEGISLAZIONE PENALE E TECNOLOGIE DELL'INFORMAZIONE: UN DIFFICILE RAPPORTO TRA CONTENITORE E CONTENUTO

Paolo Galdieri

 *Multimedia*



Clicca sull'immagine o fotografa il QrCode
per accedere al MediaBook CLIOedu

Abstract: L'Italia è dotata di una legislazione penale in materia di tecnologie dell'informazione ampia ed articolata. Sulla scia delle indicazioni dettate in ambito europeo sia rispetto al diritto positivo che processuale, sono state introdotte disposizioni in grado di contrastare la criminalità informatica. Per quanto attiene la legislazione vigente il vero problema è quello dell'interpretazione delle norme, considerato che le stesse introducono termini tecnici sinora sconosciuti ai giuristi e tenendo conto del fatto che le stesse vanno applicate a contesti sovente immateriali. Per quanto concerne la tenuta di tale legislazione, occorre, invero, riconoscere che le tecnologie evolvono ad una velocità insostenibile per il legislatore. Non resta quindi che auspicare l'impiego di norme, come avvenuto in Italia, dal contenuto più ampio possibile, lasciando all'interprete il compito di adattare le disposizioni alle nuove realtà che nel tempo possono presentarsi innanzi ai suoi occhi.

Parole chiave: società dell'informazione, tecnologie dell'informazione, Internet, reato informatico, reato telematico, indagini informatiche.

Sommario: 1. Il contributo dell'Unione Europea nella lotta ai reati informatici; 2. La legislazione penale italiana in materia di reati informatici; 3. La legislazione penale e l'evoluzione delle tecnologie dell'informazione; 4. Le questioni ancora aperte nel difficile rapporto tra legislazione penale e tecnologie dell'informazione.

1. Il contributo dell'Unione Europea nella lotta ai reati informatici

Già sul finire degli anni ottanta in ambito europeo si è focalizzata l'attenzione sui fenomeni criminali correlati all'uso delle tecnologie dell'informazione.

Di fronte all'insorgere di attività illecite realizzate attraverso sistemi informatici e telematici, si è posto il problema di comprendere se tali condotte fossero già disciplinate dalle normative interne o se fosse, viceversa, necessario, introdurre nuove disposizioni. Partendo da considerazioni sul divieto di analogia *in malam partem* e sul principio di tassatività, proprio del diritto penale, si è quindi deciso di aggiornare l'apparato normativo al fine di inserire nell'orbita del penalmente rilevante condotte altrimenti non contemplate.

L'Unione Europea, in particolare, ha da subito posto l'attenzione sul fatto che la maggior parte delle condotte correlate all'uso dei sistemi telematici, si caratterizzi per la sua natura transnazionale, rilevando che attraverso l'elaboratore, l'evento antigiuridico sovente si realizza in un luogo diverso da quello da dove è partita la condotta.

La natura transnazionale del reato informatico ha spinto, quindi, ad emanare provvedimenti in grado, da un lato, di armonizzare le legislazioni penali dei diversi Paesi membri, e, dall'altro, di uniformare le norme di procedura penale proprio al fine di favorire la cooperazione internazionale. Sul piano del diritto sostanziale documento fondamentale è rappresentato dalla raccomandazione 89/9¹ attraverso la quale viene stilata una lista, cosiddetta minima, delle ipotesi illecite particolarmente diffuse e che, quindi, dovevano essere contemplate dalle legislazioni penali di tutti gli Stati membri.

¹ V. Frosini, *Contributi ad un diritto dell'informazione*, Liguori, Napoli, 1990, p. 165 ss..

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.

Di fronte a tali indicazioni, in ambito europeo, così come avvenuto anche a livello internazionale, diversi Paesi si sono posti il problema di come intervenire in questo delicato settore. Secondo un orientamento assai diffuso in Europa i nuovi delitti non introducevano nuovi interessi meritevoli di tutela, bensì producevano soltanto nuove modalità di aggressione di beni giuridici preesistenti. Questo 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. In tale direzione si sono mosse, tra l'altro, la Danimarca, la Germania, il Lussemburgo, la Svizzera, il Portogallo e l'Italia.

Per altro indirizzo dottrinario, sviluppatosi per lo più nei Paesi anglosassoni, le nuove tecnologie determinavano l'insorgere 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 cd. legge organica).

In questa direzione si muove 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"². In ambito processuale punto di svolta è rappresentato dalla raccomandazione R 95/12 che sollecita l'armonizzazione dei codici di procedura penale, al fine di consentire l'effettiva perseguibilità dell'autore del reato. Sulla stessa scia si colloca la Comunicazione della Commissione europea "Creare una società dell'informazione sicura, migliorando la sicurezza delle infrastrutture dell'informazione e mediante la lotta alla criminalità informatica"(COM-2000-890)³ ove si individuano come temi da affrontare in modo univoco ed approfondito: a) le intercettazioni di comunicazioni; b) la conservazione dei dati relativi alle comunicazioni; c) l'accesso e utilizzo anonimi; d) la cooperazione concreta a livello internazionale; e) i poteri in materia di procedura penale e giurisdizione; f) il valore probatorio dei dati informatici.

I veri e propri pilastri della normativa di diritto sostanziale e processuale in materia di reati informatici, sono contenuti all'interno della Convenzione internazionale sul *cybercrimine* (Strasburgo, 29 giugno 2001 CDPC(2001)17), che costituisce oggi la carta fondamentale per i Legislatori di tutti i Paesi membri dell'Unione Europea.

Accanto alle indicazioni di carattere generale in materia di reati informatici, sia per quanto riguarda il diritto sostanziale che quello processuale, l'Unione Europea ha tracciato nel tempo una serie di linee guida, miranti a garantire la sicurezza della rete, anche al fine di favorire la circolazione di beni e servizi all'interno di internet.

² Il metodo delle legge organica è stato adottato negli Usa, dove 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.

³ Il testo integrale è consultabile in: www.privacy.it/com2000-890.

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, 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.

Sempre in quest'ambito, si colloca la 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.

Parimenti l'Unione Europea ha emanato una serie di provvedimenti finalizzati a limitare al massimo la diffusione dei reati nella rete. In tale direzione si muovono, oltre che la Raccomandazione del Consiglio d'Europa R (89) 9 e la Raccomandazione R (95)13, delle quali si è detto: 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.

2. La legislazione penale italiana in materia di reati informatici

L'uso illecito delle tecnologie dell'informazione è attualmente punito attraverso numerose norme penali, la maggior parte delle quali sono contenute all'interno del codice penale.

Sul piano generale si osserva come numerosi reati informatici sono stati introdotti nel codice penale attraverso la legge 23 dicembre 1993, n. 547.

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, ad esempio Stati Uniti e Francia, che hanno rispettivamente dedicato ai delitti informatici leggi *ad hoc* o un titolo apposito all'interno del codice penale, in Italia le nuove norme sono state inserite in diversi parti del codice penale, ciascuna vicino alla disposizione previgente ritenuta simile.

Vengono inseriti in primo luogo reati fino ad oggi non previsti, quali: l'accesso abusivo ad un

sistema informatico o telematico; la detenzione e diffusione abusiva di codici d'accesso; la diffusione di programmi diretti a danneggiare o interrompere un sistema informatico; il falso informatico; il danneggiamento informatico e la frode informatica.

Si procede poi all'aggiornamento di norme preesistenti al fine di renderle applicabili anche alle condotte realizzate per mezzo delle tecnologie. In tale ambito si colloca l'esercizio arbitrario delle proprie ragioni con violenza su di un bene informatico, il novellato delitto di attentato ad impianti di pubblica utilità, le intercettazioni informatiche e telematiche, la violazione di corrispondenza informatica.

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"⁴.

Nel recepire le indicazioni della Convenzione sulla Criminalità informatica, la legge 48 opera su tre piani: quello del diritto sostanziale, processuale e della rilevanza penale di alcune condotte in ambito aziendale. Quanto 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.

Interessanti modifiche si registrano 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.

Si 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 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.

Sul piano del diritto sostanziale va inoltre registrata la recente previsione dell'ipotesi di frode informatica commessa con sostituzione di identità digitale⁵, mentre in ambito procedurale viene prevista la confisca obbligatoria per i beni utilizzati per la commissione di alcuni reati informatici⁶. Accanto alla legge 547/93 si individuano altre norme riferite espressamente o comunque riferibili ai reati informatici.

La duplicazione abusiva del *software* e la commercializzazione del programma contraffatto è sanzionata penalmente dall'art. 171 *bis* della legge 22 aprile 1941, n. 633 (tale articolo è stato

⁴ Su tale argomento cfr. L. Luparia (a cura di), *Sistema penale e criminalità informatica*, Giuffrè, Milano, 2009; P.G. De Marchi (a cura di), *I nuovi reati informatici*, G. Giappichelli, Torino, 2009.

⁵ Il D.L. 14 agosto 2013 n. 93 "Disposizioni urgenti in materia di sicurezza e per il contrasto per le violenze di genere, nonché in tema di protezione civile e di commissariamento delle provincie", inserisce un terzo comma all'interno dell'art. 640 *ter* al fine di sanzionare la frode informatica commessa con sostituzione di identità digitale.

⁶ Legge 15 febbraio 2012, n. 12 "Norme in materia di misure per il contrasto ai fenomeni di criminalità informatica".

introdotto dal decreto legislativo n. 518 del 29 dicembre 1992, successivamente modificato dalla legge 18 agosto 2000, n. 248).

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.⁷.

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.⁸.

Norme penali in qualche modo riferibili a condotte correlate all'uso delle tecnologie dell'informazione sono rintracciabili anche nel "Codice in materia di protezione dei dati personali", introdotto attraverso il decreto legislativo 30 giugno 2003, n.196.

Si tratta, invero, di disposizioni non direttamente riferite all'informatica, atteso che la legge disciplina il trattamento dei dati personali, quale che sia il metodo utilizzato (tradizionale o automatizzato), ma comunque sovente applicabili al mondo informatico, considerato che la maggior parte dei trattamenti avviene mediante computer.

3. La legislazione penale e l'evoluzione delle tecnologie dell'informazione

Il rapporto che intercorre tra legislazione penale e tecnologie dell'informazione può essere rappresentato come un continuo inseguimento in cui la legge, per quanto si sforzi, non riesce mai a raggiungere la tecnologia.

Ciò non dipende, invero, da una incapacità del Legislatore di prevedere in via definitiva tutte le condotte illecite realizzabili attraverso le tecnologie, quanto piuttosto dal fatto che le stesse evolvono ad una velocità tale da rendere impossibile previsioni sugli sviluppi e conseguenze sul piano giuridico.

Se, infatti, osserviamo l'attuale legislazione penale è agevole rilevare come la stessa sul piano teorico disciplini effettivamente tutte le condotte oggi ipotizzabili.

Gli stessi fenomeni, considerati nuovi, quali il *cyberbullismo*, il *phishing*, il *cyberstalking*⁹, ed il *cyberterrorismo*¹⁰, possono essere contrastati anche con la normativa esistente, e, quindi, anche in

⁷ 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

⁸ 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

⁹ Pratica delittuosa in continua crescita è quella del cosiddetto *cyberstalking*, spesso agevolato da contesti virtuali, quali i *social networks*, che consentono a l'ex fidanzato o coniuge, o allo spasimante rifiutato, talvolta anche attraverso furti d'identità, di rendere la vita impossibile alla vittima designata. Tali condotte sono attualmente disciplinate dall'art. 612 *bis* c.p. (atti persecutori), introdotto dall'art. 7 del D.L. 23 febbraio 2009 n. 11.

¹⁰ Fenomeno più raro, ma non per questo non meritevole di attenzione, è quello del *cyberterrorismo*, riguardante l'uso delle tecnologie dell'informazione da parte dei gruppi terroristici. Per contrastare tale fenomeno, oltre alle disposizioni previste dalla legge 547/93, e quelle già presenti nel codice penale, ad esempio, nella parte dedicata ai delitti contro la personalità dello Stato, contro l'ordine pubblico e l'incolumità pubblica, di recente il legislatore ha introdotto l'art.

assenza di disposizioni ad essi esplicitamente riferite.

Sul piano del diritto positivo allora, il vero problema è quello dell'interpretazione delle norme, considerato che esse introducono termini tecnici sino a poco tempo fa non presenti nell'ordinamento giuridico e, quindi, sconosciuti ai giuristi.

Da questo punto di vista "lo sforzo" da fare è quello di assimilare le nuove nozioni, ma anche e soprattutto di acquisire una consapevolezza del modo di pensare di coloro che utilizzano le tecnologie dell'informazione. In altre parole serve una sorta di alfabetizzazione giuridico-informatica.

L'avvicinamento dell'ambito giuridico a quello informatico, consentirebbe una applicazione delle norme in grado di centrare gli obiettivi prefissati e, quindi, di contrastare con maggior forza la criminalità informatica.

Questione diversa e più complessa è quella dell'applicazione delle norme nel contesto specifico in cui le stesse sono chiamate ad operare.

È indubbio ad esempio che ogniqualvolta la norma penale, anche se non espressamente riferita alle tecnologie dell'informazione, vada applicata ad un reato commesso attraverso la rete si incontrano questioni particolari quali quelle relative all'individuazione dell'autore e del luogo del commesso reato. Ne deriva che molte delle questioni giuridiche di non facile soluzione non dipendono soltanto e soprattutto dal contenuto delle norme, quanto dal contesto in cui vengono applicate. Contesto che è bene sottolineare si caratterizza sempre più per la sua immaterialità e per il fatto che i soggetti non si incontrano fisicamente e gli eventi antiggiuridici si possono realizzare in tempo reale ed a distanza.

Innanzitutto ad un contesto sempre più immateriale, questioni giuridiche di non facile soluzione si pongono in ordine alle modalità di acquisizione, conservazione, e tenuta nel processo della prova digitale o *digital evidence*, tant'è che nel tempo si è sviluppata una disciplina specifica, denominata "*computer forensics*" o "*digital forensics*", il cui compito è proprio quello di analizzare i requisiti che deve avere il bene informatico per esser assunto come prova valida a tutti gli effetti all'interno di un processo.

Se le questioni anzidette sono strettamente interpretative ve ne sono, tuttavia, altre che, come accennato in precedenza, hanno a che fare con la velocità con la quale si modifica lo scenario caratterizzato dalle nuove tecnologie.

Quando all'inizio degli anni novanta la maggior parte dei Paesi europei decisero di dotarsi di una legislazione penale in questo settore la cosiddetta società dell'informazione era ancora in divenire. I grandi centri di calcolo erano presenti solo all'interno di importanti e strategiche strutture pubbliche e nelle aziende di grandi dimensioni e la cosiddetta alfabetizzazione informatica, caratterizzata da un utilizzo capillare del personal computer, non si era ancora realizzata in pieno. Di fronte ad uno scenario di questo tipo, il legislatore ha focalizzato la propria attenzione sulle tecnologie di fronte ad i suoi occhi e, quindi, sostanzialmente sui programmi e sui sistemi informatici e telematici, immaginando tutti i reati realizzabili attraverso o contro tali beni.

Nel volgere di pochi anni, tuttavia, la nostra società si è trasferita dal piano reale a quello virtuale

270 *ter* (articolo introdotto dalla legge 15 dicembre 2001, n. 438, che ha convertito, con modificazioni, in legge il Decreto-legge 18 ottobre 2001, n. 374, intitolato "Disposizioni urgenti per contrastare il terrorismo internazionale"), che punisce anche colui che fornisce strumenti di comunicazione ai partecipanti alle associazioni terroristiche.

e questo grazie, in un primo momento, all'utilizzo su vasta scala di Internet in tutto il mondo, successivamente, arricchendosi di contenuti nuovi rappresentati dal diffondersi dei *social networks*, che hanno aperto scenari, anche giuridici, fino a qualche anno fa impensabili.

L'utilizzo continuo della rete è stato a sua volta favorito dall'evoluzione della telefonia mobile, attraverso la quale si può veicolare qualsiasi tipo di contenuto in tempo reale.

Recentemente, infine, lo scenario si è arricchito di nuove applicazioni informatiche, quali l'internet degli oggetti¹¹ (IdO) ed il *cloud computing*¹².

L'arricchimento dei contenuti delle tecnologie ha ovviamente un riflesso su tutte le condotte umane e, quindi, anche su quelle costituenti reato.

E' ovvio che le difficoltà della legge a contenere "il nuovo che avanza" sono, talvolta, oggettive, nel senso che non tutto ciò di nuovo che arriva è sempre prevedibile sul piano normativo.

D'altra parte l'evoluzione delle tecnologie, e soprattutto del modo in cui le stesse possono essere utilizzate, pone questioni nuove non solo rispetto all'applicazione delle norme penali ed all'accertamento del reato, ma anche in relazione al modo di agire e di pensare del soggetto agente. Da questo punto di vista è agevole osservare come il mutamento del contesto ha finito con il modificare sensibilmente le motivazioni del "delinquente" informatico, considerato che l'*hacker* dell'inizio degli anni novanta era principalmente mosso da un movente politico e libertario, in sostanza contro il monopolio o l'oligopolio delle informazioni, mentre oggi esiste una vera e propria professionalità informatica nell'ambito del crimine, tant'è che esperti informatici vengono assoldati all'interno dei gruppi terroristici e dalle mafie di tutto il mondo. Il reato informatico è sempre più un reato economico, con tutte le conseguenze che si possono immaginare.

Da un po' di anni a questa parte si è compreso anche che le tecnologie dell'informazione non modificano solo il modo di agire delle persone ma anche il modo di pensare. Per quanto concerne l'ambito penale è interessante notare come ormai da anni si parli di dipendenza da internet equiparata a psicopatologie quali la bulimia ed il gioco d'azzardo, e sempre più diffuse sono le cosiddette "droghe tecnologiche".

Una nuova frontiera del diritto da qui a breve potrebbe essere quella che analizza le ripercussioni sulla mente umana della mediazione tecnologica, al fine di verificare se ciò possa avere una ricaduta sull'interpretazione di alcuni istituti, quali l'imputabilità, i motivi a delinquere, ecc.

4. Le questioni ancora aperte nel difficile rapporto tra legislazione penale e tecnologie dell'informazione.

Nel rapporto legislazione penale – tecnologie dell'informazione è possibile individuare due ordini di problemi. Il primo si riferisce all'interpretazione delle disposizioni di diritto positivo e

¹¹ L'Internet degli oggetti, chiamato anche informatica "ubiquitaria" o "intelligenza ambientale", comprende determinate tecnologie (R.f.i.d., TCP/IT, Bluetooth, ecc), che collegate insieme consentono di identificare oggetti, raccogliere dati, trattarli e trasferirli.

¹² Si tratta di una nuova metodologia della struttura IT tramite la banda larga, concretandosi in una automazione dei servizi di gestione.

processuale, resa difficoltosa dal fatto che le norme inseriscono termini tecnici sino a poco tempo fa sconosciuti ai giuristi e considerato che si applicano a contesti di regola immateriali. Quanto a quest'ultimo aspetto, tema centrale è quello di uno sviluppo della disciplina della cosiddetta “*digital forensic*”, tale da fornire regole il più possibile omogenee in tema di acquisizione, analisi e conservazione della prova digitale.

Problema differente è quello relativo alla tenuta della legislazione penale di fronte al continuo evolvere delle tecnologie.

Da questo punto di vista è agevole rilevare come, inevitabilmente, la norma penale non sempre sembrerà in grado di contrastare le condotte “tecnologiche” e ciò non solo per le diverse modalità di agire in concreto ipotizzabili, ma soprattutto perché le tecnologie stesse evolvono ad una velocità tale, non sempre prevedibile per il Legislatore.

Di fronte a tale situazione, tuttavia, la soluzione del problema non può essere sicuramente quella di legiferare ogniqualvolta si “affaccia” nella società un nuovo prodotto informatico od una nuova applicazione. Tale strada porterebbe, infatti, ad una sorta di legislazione “emergenziale” ed emotiva che piuttosto che colmare le lacune finirebbe con il creare un sistema normativo disordinato e caotico.

Preferibile è invece percorrere la strada di una legislazione razionale, capace di produrre norme in grado di contenere i termini tecnici più ampi possibili, così da far rientrare anche beni che costituiscono una evoluzione di quelli per i quali si era previsto di legiferare.

E' ovvio che tale opzione presuppone una maggiore responsabilità dell'interprete, il quale dovrà essere in grado di adeguare le disposizioni alla nuova realtà innanzi ai suoi occhi.

Sarebbe allora utile richiamarsi all'insegnamento di Vittorio Frosini per il quale: “*il compito di noi giuristi è quello di recuperare quanto più possiamo le passioni e gli interessi degli uomini, che appartengono alla sfera dell'irrazionalità, cioè dell'immediatezza emozionale, del tornaconto particolare, portandole nella sfera assai più umana, ossia più civile e più ordinata della ragionevolezza giuridica, in cui l'azione viene mediata dai simboli delle norme*”¹³.

¹³ V. Frosini, *Informatica, diritto, società*, II Ediz. ampliata, Milano Giuffrè, 1992, pag. 160.

FIRME GRAFOMETRICHE E TUTELA DEI DATI PERSONALI

Gianluigi Ciacci

 *Multimedia*



Clicca sull'immagine o fotografa il QrCode
per accedere al MediaBook CLIOedu

Abstract: Nell'ambito del sistema italiano di validazione giuridica delle dichiarazioni elettroniche di recente si è affermata una nuova modalità di sottoscrizione in forma elettronica, quella delle c.d. firme grafometriche: modalità che è stata ritenuta inquadabile tra le c.d. firme elettroniche avanzate secondo quanto stabilito dal Codice dell'Amministrazione Digitale e dalle nuove regole tecniche emanate con il D.P.C.M. 22 febbraio 2013. Le firme grafometriche sono quelle che utilizzano il rilevamento dinamico dei dati calligrafici (posizione, pressione, velocità, tempo, inclinazione della penna, accelerazione, movimento, ...) della sottoscrizione di un individuo, acquisiti attraverso una penna elettronica, o comunque attraverso un tablet. Ma proprio il fatto di basarsi sull'acquisizione di informazioni di tipo comportamentale, e quindi di dati biometrici, rende questo nuovo sistema sottoposto alla disciplina del D.Lgs. 30 giugno 2003 n. 196, il Codice in materia di protezione dei dati personali: con una serie di criticità che vengono esaminate nel presente scritto, rielaborazione dell'intervento al Convegno dell'A.N.D.I.G. "I nuovi scenari della società dell'informazione: aspetti politici, giuridici, amministrativi e tecnici" tenuto a Roma il 29 ottobre 2013.

Recently a new type of electronic signature known as the "Graphometric Signature" has a growing relevance in Italy. It consists of a handwritten signature being added to a digital document by means of a tablet using a special pen. According to the Italian Digital Administration Code currently in force, and the new technical rules on electronic signatures issued with D.P.C.M. 22 febbraio 2013, this signature can be regarded as either an electronic signature or as an advanced electronic signature. This technology saves the signature, digitally, but at the same time special sensors gather every detail of how a person actually signs its name: the speed, writing angle, pressure and even the rhythm of a person's signature is recorded, making it unique to each person and virtually impossible for the signature to be forged.

The technology used in graphometric signature systems involves the processing of biometric user data, and then it must be applied the Italian Data Protection Code. This article examines criticality and problems of this application, analyzing recent decisions by the Italian Data Protection Authority concerning preliminary examination of these systems.

Parole chiave: documento elettronico, firme elettroniche, firme grafometriche, biometria, dati biometrici, protezione dei dati personali, Garante privacy, verifica preliminare

Sommario: 1. La gestione dell'attività di documentazione in forma elettronica e il suo valore giuridico. 2. La sottoscrizione elettronica mediante la firma grafometrica: caratteristiche, utilità, tipologie e valore giuridico. 3. Le firme grafometriche come firme biometriche: la biometria e protezione dei dati personali. 4. Le pronunce del Garante per la protezione dei dati personali sui sistemi di firme grafometriche.

Il tema delle firme grafometriche si inserisce nel settore di studi relativo al valore giuridico del documento informatico, nato nel nostro Paese negli anni '80 e consolidatosi nella seconda metà degli anni '90 con l'introduzione del sistema di firma digitale (era il 1997) allo scopo di sottoscrizione elettronica. Firma digitale che si basava (in maniera trasparente per l'utente) sulla crittografia asimmetrica per acquisire certezza della provenienza, dell'imputazione di una determinata dichiarazione elettronica, e sulla c.d. funzione di hash per raggiungere il risultato della non ripudiabilità del testo, del contenuto di tale dichiarazione elettronica. L'applicazione di entrambe le tecniche permetteva quindi di equiparare, dal punto di vista del valore giuridico, il

documento elettronico firmato digitalmente al tradizionale documento cartaceo sottoscritto in maniera autografa.

Sedici anni dopo, a fronte della enorme diffusione delle tecnologie informatiche e telematiche, della sempre più affermata smaterializzazione dell'attività di documentazione, si è sentita la necessità di andare oltre, di superare la tecnologia della firma digitale (anche in conseguenza dell'evoluzione normativa di spinta comunitaria), e si sono create nuove e diverse modalità di sottoscrizione elettronica, come appunto quella delle firme grafometriche.

Queste sono una particolare tipologia di firma con strumenti informatici che utilizza il rilevamento dinamico dei dati calligrafici (posizione, pressione, velocità, tempo, inclinazione della penna, accelerazione, movimento,...) della sottoscrizione di un individuo, acquisiti attraverso una penna elettronica, o comunque attraverso un tablet. Tipologia che sta avendo di recente una repentina diffusione, tra l'altro perché consente di essere utilizzato senza nessuna preventiva predisposizione al sistema, e quindi senza costi, per il soggetto che firma.

Ma l'assenza di costi, e la maggiore facilità di utilizzo e gestione, non esime l'utente di tale metodologia dalla necessità di coordinare la propria iniziativa con specifiche discipline di settore ad essa in qualche modo collegate. Questo non solo per le fonti appositamente dedicate alla fattispecie (da ultimo il DPCM 22 febbraio 2013, le regole tecniche sulle firme elettroniche), ma con particolare riferimento alla normativa in materia di tutela dei dati personali, il D.Lgs. 30 giugno 2003 n. 196, poiché l'utilizzo delle firme grafometriche implica il trattamento di informazioni relative all'individuo: e quindi porta all'applicazione di quell'insieme di regole, spesso oscure e contraddittorie, che rientrano nella c.d. (seppure imprecisamente) "legge sulla privacy".

Nel presente scritto, premesso un breve approfondimento circa la tematica del valore giuridico del documento elettronico, delle firme elettroniche e delle firme grafometriche, affronteremo il problema dell'applicazione delle disposizioni del D.Lgs. 196/2003 al settore in esame, anche alla luce di alcune recenti pronunce dell'Autorità Garante per la protezione dei dati personali.

1. La gestione dell'attività di documentazione in forma elettronica e il suo valore giuridico.

Come si è detto, alla fine degli anni ottanta in Italia la sempre maggiore diffusione dell'informatica nei più diversi settori della collettività ha reso necessario stabilire quale valore giuridico dovesse essere riconosciuto all'attività di documentazione svolta in modo elettronico. Infatti, i principali istituti giuridici che venivano in modo più o meno spontaneo applicati ed osservati nella quotidianità erano stati concepiti per una realtà materiale, che tradizionalmente era quella cartacea, nella quale si riteneva necessaria la sottoscrizione autografa per ottenere l'imputazione di una determinata dichiarazione: elementi che rendevano possibile verificare la presenza dei requisiti di genuinità, sicurezza, provenienza e non ripudiabilità in un documento, necessari a dare ad esso una rilevanza giuridica. Dopo un intenso dibattito, ed un lungo periodo di studio e quindi di consolidamento della tematica, la soluzione che si è scelta di adottare nella seconda metà degli anni novanta per dare valore al documento elettronico è stata quella dell'adozione della c.d. firma digitale: sistema che ha visto dare rilevanza ad un procedimento puramente tecnico nell'ambito di una disciplina di

tipo giuridico per ottenere il risultato richiesto.

Per “firma digitale”, in particolare, si deve intendere la sottoscrizione predisposta mediante elaboratore elettronico sulla base della tecnica della crittografia a chiave asimmetrica (anche detta a doppia chiave) e di una particolare funzione matematica (la c.d. funzione di hash): con la prima si raggiunge la certezza della provenienza della dichiarazione elettronica; con la seconda tecnica si ottiene invece la sicurezza che il testo della dichiarazione non sia stato alterato, che sia dunque integro, e di conseguenza non ripudiabile. Niente a che vedere quindi con la tradizionale sottoscrizione posta alla fine, o a margine, di un foglio di carta, né proprio con la firma autografa: in questo caso si tratta infatti di un sistema puramente tecnico che si basa sull’esclusività del suo uso, e non sull’univocità della calligrafia di firma, per rendere possibile l’imputazione di un documento elettronico. Sistema che costituisce oggi il criterio legale in base al quale è possibile far risalire ad un determinato soggetto un documento redatto attraverso il computer: criterio mediante il quale cioè l’ordinamento giuridico riesce ad attribuire il valore di piena prova alla documentazione prodotta, gestita e trasmessa utilizzando le nuove tecnologie dell’informazione e della comunicazione, prescindendo dalla necessità della relativa stampa, e quindi della relativa sottoscrizione autografa.

Risolto in questo modo il problema relativo all’efficacia dell’uso dell’informatica nell’attività di documentazione, negli anni successivi in diverse occasioni il Legislatore è intervenuto per modificare differenti aspetti del sistema italiano di validazione giuridica del documento elettronico: modifiche a livello tecnico (apertura a diverse tipologie di firme elettroniche oltre a quella digitale, quali la firma elettronica semplice, quella avanzata, quella qualificata) o giuridico (creazione di differenti valenze per le diverse realtà di documenti elettronici, a seconda della presenza o meno di una firma, e del tipo di questa), fino ad arrivare ai giorni nostri, in cui si può considerare abbastanza consolidata la situazione. Infatti, tralasciando la descrizione dell’indicata evoluzione normativa del sistema, oggi è possibile individuare sia gli strumenti per procedere nella sottoscrizione elettronica (ad esempio di una mail o di un modulo da compilare all’interno di un sito web), sia le diverse fattispecie legate al valore giuridico del documento elettronico, che si possono schematizzare in questo modo: con riferimento alle tipologie di firma, senza dilungarci nella precisa descrizione tecnica di ognuna di esse, si possono distinguere

- *la firma elettronica (semplice)*, di cui può costituire esempio la digitazione del pin del bancomat insieme alla lettura della corrispondente tessera magnetica (per farsi riconoscere titolare del conto corrente bancario), o ancora il nome-utente e la password per accedere ad un determinato servizio (come nel caso di utilizzo della posta elettronica): si tratta di dati elettronici associati ad altri dati, ed utilizzati come metodo di identificazione informatica (la definizione completa è riscontrabile nell’art. 1, lett. q, del D.Lgs. 82/2005, il c.d. C.A.D., Codice dell’Amministrazione Digitale).
- *la firma elettronica avanzata (F.E.A.)*, di cui oggi sembrerebbero rappresentare principale esempio le applicazioni di *firma grafometrica*, quelle cioè che vedono l’apposizione di una sottoscrizione autografa su tavoletta elettronica, in grande sviluppo soprattutto nel settore bancario: come si vedrà in maniera approfondita oltre, anche per la presente tipologia si tratta di dati in forma elettronica allegati, o comunque connessi, ad un documento informatico, creati con mezzi sui quali il firmatario ha un controllo esclusivo, che consentono la sua identificazione e allo stesso tempo di rilevare se gli stessi dati firmati siano stati successivamente modificati (anche in

questo caso si veda per la definizione precisa l'art. 1, lett. *q/bis*, del C.A.D.). Di recente alcune applicazioni di firma grafometrica, oltre ad identificare l'autore della sottoscrizione elettronica, consentono anche di ottenere l'imputazione della dichiarazione al suo autore, utilizzando tecniche proprie della successiva tipologia.

- *la firma elettronica qualificata*, di difficile individuazione autonoma dalla firma digitale, di cui al successivo punto, è una firma elettronica avanzata che utilizza dispositivi sicuri per la realizzazione della sottoscrizione elettronica, con l'intervento di società di certificazione di alto livello (per la definizione si veda l'art. 1, lett. *r* del C.A.D.): ne possono costituire esempi i sistemi di gestione a distanza dei rapporti bancari attraverso l'identificativo utente e il c.d. token, ed anche le applicazioni di firma grafometrica che uniscono agli strumenti di identificazione dell'autore anche quelli di imputazione certa della sua dichiarazione, ad esempio in campo sanitario per l'acquisizione del consenso informato medico.
- *la firma digitale*, che tra le varie tipologie è quella più affermata e consolidata (nel 2013 si sono raggiunti i 7 milioni di kit per firmare digitalmente distribuiti nel nostro Paese), è il ricordato sistema che utilizza la crittografia asimmetrica e la funzione di hash per raggiungere la certezza dell'autore della dichiarazione elettronica e la non ripudiabilità della stessa: al momento è possibile acquisirla da una decina di certificatori (tra cui Postecom, Aruba, Infocert, Actalis,...), con una spesa media annua di circa cinquanta euro, e si può utilizzare per diverse necessità, dalla partecipazione a concorsi pubblici, all'invio della dichiarazione dei redditi, alla notifica del trattamento dei dati personali al Garante della privacy.

Con riferimento ai diversi valori giuridici conseguibili usando, o meno, le indicate modalità di sottoscrizione elettronica (valori che in genere si rapportano all'idea di valutazione da parte di un giudice, e quindi ad una fase conflittuale del rapporto tra le parti, ma che chiaramente possono essere riferiti a situazioni operative e precedenti, o comunque che prescindono dal sorgere di una controversia), sulla base della disciplina dettata dagli artt. 20 e 21 del C.A.D. distinguiamo

- *documento elettronico predisposto senza una firma elettronica*: nel caso in cui tale documento si riferisca in qualche modo al suo autore (si pensi ad un form in cui viene compilato con i dati di chi lo invia), il suo valore è assimilabile a quello di prova legale se non viene disconosciuto dalla parte contro cui è prodotto, altrimenti sarà liberamente valutabile dal giudice che terrà conto delle caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità del documento; *in pratica*, questo ha un suo valore di per sé, e in caso di contestazione nel rapporto può essere prodotto in giudizio come succede per quello cartaceo (anche se poi sarà probabilmente oggetto di controversia proprio la sua genuinità: cioè la parte che ha mandato il documento potrebbe negare di averlo fatto, o di averlo fatto con quel testo, spostando quindi l'onere di provarne l'autore al soggetto che l'ha ricevuto).
- *documento elettronico predisposto con una firma elettronica semplice*: anche in questo caso sarà la libera valutazione del giudice (che terrà conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità) a stabilirne il valore; rispetto al caso precedente si restringerebbe l'ambito di discrezionalità connesso al convincimento del giudice, perché il documento firmato, seppure con una firma-base, avrebbe un maggior grado di affidabilità. *In pratica*, l'aver previsto un sistema di sottoscrizione elettronica rende più semplice la gestione dell'eventuale azione giudiziaria di contestazione.
- *documento elettronico predisposto con una firma elettronica avanzata, qualificata o digitale*: in questo caso

si realizza la totale equiparazione tra documento cartaceo ed informatico, tra sottoscrizione autografa ed elettronica, ed in particolare il valore che si attribuisce, secondo quanto previsto dall'art. 21 comma 2 del C.A.D., è quello ex art. 2702 del codice civile, quindi di scrittura privata (che fa piena prova della provenienza della dichiarazione da chi l'ha sottoscritta). La differenza tra l'uno o l'altro tipo di firma, a parte le specifiche tecniche già indicate, influenza gli atti che devono essere firmati, e non il valore giuridico in sé: infatti per situazioni giuridiche particolarmente rilevanti (ad esempio, la compravendita di un immobile, o per gli atti previsti nell'art. 1350 nn. 1-12), è necessaria la firma più sicura, e quindi quella digitale, o comunque qualificata; per atti giuridici di rilevanza minore (ad esempio, un contratto di assicurazione o il patto di non concorrenza, atti previsti dall'art. 1350 n. 13) è sufficiente una firma elettronica avanzata. *In pratica*, se sorge una controversia, e viene prodotto in giudizio un documento elettronico a cui è stata apposta una firma digitale, o comunque una firma elettronica avanzata, il suo valore è assimilabile a quello di prova legale (se non viene disconosciuto dalla parte contro cui è prodotto: ipotesi in cui sarà però tale parte a dover dimostrare il motivo per cui il documento non gli si può imputare, e se non ci riesce si realizza la prova legale, cioè viene riconosciuto provato quanto affermato dalla parte che lo ha prodotto in giudizio): il giudice non sarà quindi più libero di valutare o meno affidabile quel documento, ma è obbligato a considerarlo come una scrittura privata.

Indicati i punti più rilevanti degli aspetti legali dell'attività di documentazione attraverso le nuove tecnologie dell'informazione e della comunicazione, si procederà ora ad esaminare una nuova applicazione di sottoscrizione elettronica, la firma grafometrica, che di recente ha avuto una rilevante diffusione nel nostro Paese. Diffusione che sicuramente dipende dalle sue caratteristiche (facilità ed economicità d'uso, ma soprattutto nessun onere per il soggetto che firma), ma che è anche legata al suo riconoscimento normativo, sia come sistema di sottoscrizione elettronica valido (rientrerebbe nella tipologia di firma elettronica avanzata introdotta dall'art. 1, comma 1, lett. q-bis del D.Lgs. 82/2005), sia in particolare come metodologia adatta alla sottoscrizione di una serie di atti giuridici individuati sulla base dell'art. 1350 n. 13 del codice civile.

2. La sottoscrizione elettronica mediante la firma grafometrica: caratteristiche, utilità, tipologie e valore giuridico.

Come si è detto, la firma grafometrica è quella particolare tipologia di firma con strumenti informatici che utilizza il rilevamento dinamico dei dati calligrafici della sottoscrizione di un individuo (e quindi la posizione della penna, la sua inclinazione, la pressione del segno grafico, la velocità del movimento, la sua accelerazione, il tempo complessivo,...), acquisiti attraverso una penna elettronica, o comunque attraverso un tablet.

In tale sistema il soggetto che firma non dovrà preventivamente dotarsi di alcun dispositivo tecnico, evitando da una parte di doverne sostenere i costi, dall'altra di affrontare le complicazioni gestionali normalmente connesse all'utilizzo degli strumenti necessari ai medesimi scopi (ad

esempio per munirsi di un dispositivo di firma elettronica qualificata, o di firma digitale; poi per conservarlo in maniera sicura nel tempo; infine, per ricordarsi di “portarselo dietro” nel momento in cui si decida di utilizzarlo, rendendo quindi praticamente impossibili utilizzi estemporanei dello stesso): molto semplicemente, in alcune situazioni (ad esempio in banca, oppure alla reception di un albergo o alla cassa di un negozio, o ancora in altre specifiche realtà, come nel caso di consegne postali, o per la sottoscrizione del consenso informato medico), ci si troverà davanti ad una tavoletta grafica con penna elettronica, oppure ad un tablet con pennino, e si procederà a sottoscrivere un determinato testo apparso a video, di cui si è presa visione, praticamente come se si utilizzassero i tradizionali strumenti della carta e della penna.

Chi dovrà attivarsi per dotarsi dei dispositivi di firma, e per organizzare sotto diversi punti di vista un sistema di firma grafometrica, sarà chi vuole usufruire dei vantaggi di tale tecnologia (che sono diversi e di rilevante importanza, come si vedrà oltre): così, ad esempio, la banca, l'albergo, il negoziante o il medico che deve raccogliere il consenso informato del proprio paziente per iscritto. Soggetti che dovranno svolgere un'attività di predisposizione della propria struttura che implica certamente la necessità di occuparsi da una parte di diversi aspetti tecnici (dalla scelta del fornitore del sistema, alla decisione relativa alla finalità che si vuole raggiungere, ...), e dall'altra di alcune procedure giuridiche, in particolare conseguenza del fatto che i dati grafometrici sono di natura biometrica, come si approfondirà nel successivo capitolo.

Con riferimento alle utilità collegate all'uso di questa tipologia di firma, a parte quanto già riportato nella descrizione delle caratteristiche del sistema, e quindi la maggiore semplicità per colui che firma (specifica che le rende adatte a certe necessità, e non ad altre: ad esempio, è inutile nel caso i soggetti debbano sottoscrivere documenti informatici occasionalmente e a distanza, mentre è molto utile per le sottoscrizioni da porre in essere “in presenza”), si può rilevare la migliore efficacia rispetto ai tradizionali e corrispondenti sistemi “analogici”, cartacei. Infatti, secondo quanto riportato dalle società che forniscono sistemi di sottoscrizione grafometrica, nel caso di accertamento periziale su un documento cartaceo firmato in maniera autografa da un soggetto, le percentuali “di vero”, cioè la possibilità di acquisire la certezza circa l'autenticità della sottoscrizione è pari al 60-65 %; mentre, nel caso si debba procedere ad un simile accertamento di una firma grafometrica su un documento informatico la percentuale di vero è superiore, nella specie intorno al 90-95 % (risultato conseguito perché all'analisi tradizionale a livello grafico del perito si sommano gli altri parametri resi possibili da specifici software che agiscono nel sistema). Quindi risulta essere più “sicura” una firma realizzata con l'ausilio di tale tecnologia rispetto a quella tradizionale analogica.

Deve essere infine considerato anche il minore costo complessivo del sistema: se infatti il soggetto che riceve le sottoscrizioni, e che dunque adotta il processo di firma grafometrica, sosterrà una spesa superiore, sarà però l'unico ad essere gravato di un costo (e comunque tale costo verrà bilanciato dal maggiore vantaggio, anche economico, conseguito a causa dell'esponenziale aumento del numero di soggetti che firmeranno i suoi documenti informatici), non dovendo spendere nulla il soggetto che invece firma.

Al momento le firme grafometriche vengono utilizzate, in tale ambito, con due diverse finalità, rispetto alle quali variano anche le modalità di uso dei relativi dati grafometrici:

- *a fini di identificazione*, di autenticazione: è la metodologia attualmente più diffusa, la sottoscrizione grafometrica viene utilizzata per riconoscere il soggetto che firma, in modo da consentirgli

di realizzare un determinato scopo (come ad esempio l'effettuazione di un bonifico dal proprio conto presso un istituto bancario). In essa le informazioni grafometriche (cioè quelle corrispondenti al rilevamento dinamico dei dati calligrafici della firma dell'individuo) acquisite grazie al dispositivo di firma sono accessibili dal soggetto che riceve la firma, e da questo conservate, poiché devono essere ogni volta confrontate con l'originario *spécimen*: il soggetto che fa firmare, e quindi riceve e conserva quei dati (ad esempio una banca), può dunque accedere, e di fatto accede, sia al dato grafometrico originario, sia a quello creato nella specifica occasione (entrambi parametri per effettuare il confronto e procedere nell'identificazione);

- *a fini di imputazione*, dichiarativi: è la metodologia che negli ultimi mesi sta avendo un forte sviluppo, in cui la sottoscrizione grafometrica è utilizzata per ricondurre una dichiarazione elettronica ad un determinato soggetto, suo autore (ad esempio, per acquisire l'accettazione di un'offerta contrattuale, oppure per raccogliere il consenso informato ad una prestazione sanitaria). Il funzionamento è diverso dalla precedente ipotesi: infatti i dati grafometrici non sono disponibili al soggetto che riceve la firma, il cui interesse all'accesso è solo eventuale, e unicamente nel caso il firmatario contesti di aver sottoscritto la determinata dichiarazione elettronica (ad esempio, il modulo del consenso informato alla prestazione sanitaria, oppure la dichiarazione di accettazione negoziale). In tale applicazione interviene una terza parte, che svolge il compito di rendere inaccessibile il dato grafometrico al soggetto che lo detiene, usando la tecnica della crittografia asimmetrica, ed eventualmente renderlo di nuovo accessibile nel momento in cui si attivi una procedura giudiziaria (ipotesi quindi legata ad un preciso ordine dell'autorità giudiziaria che richieda appunto l'acquisizione del dato): così in tale utilizzo si verifica la situazione che vede il soggetto che detiene il dato grafometrico non in grado di accedervi perché criptato, mentre il soggetto che ha la possibilità di decriptarlo non ha però la disponibilità del dato.

Con riferimento al valore giuridico delle firme grafometriche, innanzitutto esse possono essere pacificamente considerate quali firme elettroniche (semplici), e dunque come indicato in precedenza il loro valore è quello di prova legale se non vengono disconosciute dalla parte contro cui sono prodotte; in caso contrario, il livello probatorio sarà liberamente valutabile dal giudice che terrà conto delle caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità del documento firmato con lo strumento grafometrico. Ma le firme grafometriche possono essere considerate anche quali firme elettroniche avanzate ai sensi dell'art. 1, lett. *q/bis*, del C.A.D., e con il valore probatorio stabilito dal suo art. 21 (scrittura privata ex art. 2702 del codice civile) ?

Per rispondere a questa domanda occorre fare riferimento a quanto disposto dal D.P.C.M. 22 febbraio 2013, le "Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali (...)", il cui art. 56 elenca le caratteristiche che deve avere una soluzione F.E.A. per essere considerata tale. In particolare, i requisiti ritenuti necessari sono:

l'identificazione del firmatario del documento, la connessione univoca della firma al firmatario, il controllo esclusivo del firmatario del sistema di generazione della firma (ivi inclusi i dati biometrici eventualmente utilizzati per la generazione della firma medesima), la possibilità di verificare che l'oggetto della sottoscrizione non abbia subito modifiche dopo l'apposizione della firma, la possibilità per il firmatario di ottenere evidenza di quanto sottoscritto, l'individuazione del soggetto di cui all'art. 55 comma 2 lettera *a* (n.d.r., cioè chi commercializza la soluzione di firma

grafometrica), l'assenza di qualunque elemento nell'oggetto della sottoscrizione atto a modificarne gli atti, fatti o dati nello stesso rappresentati, la connessione univoca della firma al documento sottoscritto.

A fronte dunque dell'applicazione del principio di neutralità tecnologica stabilito per la firma elettronica da parte del C.A.D., in base al quale non viene richiesto l'utilizzo di una determinata tecnologia per realizzarla, se la specifica soluzione adottata corrisponde a quanto previsto dall'art. 56 delle citate regole tecniche, la risposta al quesito sarà affermativa: e quindi sarà possibile considerare come firma elettronica avanzata la firma grafometrica, e sottoscrivere con tale modalità gli atti individuati sulla base dell'art. 1350, n. 13, del codice civile (ad esempio un contratto di assicurazione, il compromesso che demanda una controversia alla soluzione arbitrale, il consenso informato al trattamento sanitario,...).

Individuato il fondamento giuridico all'uso di tale soluzione tecnica, a fronte della sua indubbia utilità pratica ed efficacia tecnologica, occorre a questo punto analizzare un ulteriore aspetto del processo di sottoscrizione grafometrica che solleva diverse difficoltà: questa volta non tanto rispetto alla disciplina del valore giuridico del documento elettronico, quanto per il differente settore della protezione dei dati personali del firmatario. Infatti, il ricordato rilevamento dinamico dei dati calligrafici (posizione, pressione, velocità, tempo, inclinazione della penna, accelerazione, movimento, ...) della sottoscrizione di un individuo, portando all'acquisizione di informazioni di tipo comportamentale su quell'individuo, e quindi di tipo biometrico, realizza appunto un trattamento di dati biometrici, disciplinato in maniera specifica dal D.Lgs. 30 giugno 2003 n. 196, il Codice in materia di protezione dei dati personali.

3. Le firme grafometriche come firme biometriche: la biometria e protezione dei dati personali.

Per comprendere appieno il motivo per cui anche in questa fattispecie di sottoscrizione elettronica si debba applicare la disciplina in materia di dati personali, occorre muoversi dal concetto di "biometria", o meglio di dato biometrico. Devono infatti considerarsi tali le proprietà biologiche, gli aspetti comportamentali, le caratteristiche fisiologiche, i tratti biologici o le azioni ripetibili laddove tali caratteristiche e/o azioni sono tanto proprie di un certo individuo quanto misurabili, anche se i metodi usati nella pratica per misurarli tecnicamente comportano un certo grado di probabilità (definizione riportata nel parere del Gruppo art. 29 n. 3/2012 sugli sviluppi nelle tecnologie biometriche adottato il 27 aprile 2012): ne costituiscono esempi le impronte digitali, l'impronta retinica, l'analisi del DNA, il riconoscimento del volto o dello schema delle vene, e, tra gli aspetti comportamentali, proprio le firme grafometriche. Più nel dettaglio, il dato biometrico presenta tre caratteristiche del tutto peculiari: l'*universalità*, posto che l'elemento biometrico è presente in ciascun individuo; l'*unicità*, atteso che la componente biometrica è distintiva di ogni persona; la *permanenza*, dato che ognuno tendenzialmente conserva la propria caratteristica biometrica nel tempo.

Le tecnologie biometriche sono strettamente connesse a talune qualità personali degli individui, essendo i dati biometrici direttamente collegati al soggetto, alcune delle quali possono essere

utilizzate anche per rilevare dati sensibili (ne costituisce esempio il riconoscimento del volto, che permette di acquisire l'origine razziale del soggetto ritratto): molte di esse permettono poi anche il tracciamento automatizzato, nonché la profilazione delle persone, per cui il loro impatto potenziale sulla vita privata e sulla protezione dei dati delle persone è elevato. Si distinguono, in tale ambito, tecniche di tipo fisico e fisiologico (come per la verifica delle impronte digitali, l'analisi della retina, il riconoscimento del volto, della geometria della mano o della forma dell'orecchio, il rilevamento dell'odore del corpo, il riconoscimento vocale, l'analisi della struttura del DNA, ...), di tipo comportamentale (ad esempio la verifica della firma manoscritta, l'analisi dell'andatura, il modo di camminare o di muoversi, schemi che indicano percorsi mentali subconsci come il fatto di mentire,...), ed infine quelle basate sulla psicologia, settore emergente in cui rientra la misurazione della risposta a situazioni concrete o test specifici per l'eventuale corrispondenza a un determinato profilo psicologico.

È importante ancora distinguere tra identificazione e autenticazione biometrica. Nel primo caso si è in presenza di un processo in forza del quale un sistema riconosce un individuo, e ne accerta l'identità, confrontando i dati del medesimo con una serie di modelli biometrici: dando, quindi, risposta alla domanda: "Chi è Tizio?". L'autenticazione biometrica è invece il processo finalizzato a verificare che l'incaricato che chiede di accedere ad un determinato sistema sia effettivamente colui che dichiara di essere, attraverso il confronto dei suoi dati biometrici con quelli di un unico modello: dando, quindi, risposta alla domanda: "Tizio è la persona che dichiara di essere?".

Il trattamento dei predetti dati richiede elevate cautele per prevenire possibili pregiudizi a danno degli interessati. Ma questo non significa che, in via generale, la normativa in materia ne impedisca l'utilizzo: stabilisce invece gli ambiti di trattamento consentiti in determinate condizioni, e le modalità concrete di questo, facendo rientrare tale tipo di trattamento di dati nei parametri tipici della stessa disciplina, applicando in particolare i principi generali della stessa.

Così, la finalità del trattamento è considerato un requisito fondamentale per il ricorso alla biometria: consiste nella chiara definizione degli scopi per i quali vengono raccolti e trattati i dati, tenendo conto dei rischi per la protezione dei diritti fondamentali e delle libertà delle persone. Anche con riferimento al principio di proporzionalità, deve essere valutata ogni categoria di dati trattati alla luce delle finalità del trattamento, considerando una serie di fattori: se il sistema è essenziale per soddisfare tale necessità o, piuttosto, se è solo il più conveniente; se il conseguente aumento della possibilità di lesione del dato personale sia proporzionata al vantaggio previsto; se esista un mezzo potenzialmente meno lesivo, o comunque meno invasivo della riservatezza, che possa raggiungere lo scopo desiderato. Il rispetto poi del principio di accuratezza implica l'attenzione al fatto che i dati biometrici trattati debbano essere accurati e pertinenti rispetto alle finalità per le quali vengono rilevati. E l'applicazione di quello di "minimizzazione dei dati", alla luce del fatto che spesso i dati biometrici contengono più informazioni di quelle richieste per il confronto delle funzioni, porta il titolare del trattamento biometrico a prestare attenzione, da una parte, a che soltanto le informazioni richieste debbano essere trattate, trasmesse o conservate, e non tutte quelle disponibili; e, dall'altra, che la configurazione di partenza del sistema biometrico agevoli la protezione dei dati.

Anche con riferimento alla durata del trattamento si applicano le regole generali: così, il titolare deve determinare un periodo di conservazione per i dati biometrici che non dev'essere superiore a quello necessario al conseguimento delle finalità per le quali essi sono rilevati o sono successivamente trattati; al termine del quale deve essere garantito che le informazioni o i profili derivati da tali

dati siano cancellati definitivamente (differenziando tra i dati generici che può conservare, e quelli biometrici non più utili che deve cancellare).

A parte l'applicazione dei principi generali della disciplina in materia di protezione delle informazioni personali, il trattamento dei dati biometrici implica la necessità di adeguarsi ad alcune sue previsioni specifiche, adempiendo ai rispettivi obblighi.

Infatti per il Codice in materia di protezione dei dati personali l'utilizzo delle informazioni biometriche deve essere inteso come un'attività "che presenta rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato", a cui quindi si applica il disposto del suo art. 17: e dunque chi vuole procedere in questo tipo di attività deve sottoporre a verifica preliminare dell'Autorità Garante per la protezione dei dati personali la sua intenzione. Verifica che verterà sulla presenza di quei requisiti che si sono indicati in precedenza.

Superata la verifica preliminare dell'Autorità (tenendo presente che, secondo il Provvedimento dell'8 aprile 2010 in tema di videosorveglianza, il Titolare è espressamente esonerato dal c.d. *prior checking* qualora il Garante si sia già espresso con un provvedimento di verifica preliminare in relazione a determinate categorie di titolari o di trattamenti) occorrerà procedere alla notifica dell'attività di trattamento alla medesima Autorità sulla base dell'art. 37, e quindi porre in essere gli altri adempimenti previsti dal D.Lgs. 196/2003. In particolare, predisporre e somministrare l'esplicita informativa al soggetto i cui dati si vogliono trattare, ed acquisirne il consenso, organizzando comunque modalità alternative in caso di rifiuto di tale consenso. Tutto questo tenendo presente che le sanzioni, in caso di inosservanza di tali specifiche previsioni, sono di notevole entità. Nella specie, la mancata richiesta di verifica preliminare è sanzionata, se dal fatto deriva documento, con la reclusione da uno a tre anni, e comunque con il pagamento di una somma da 10.000 a 120.000 euro e (così gli artt. 167, comma 2, e 162, comma 2-*bis*, del D.Lgs. 196/2003); ed anche la mancata notificazione ha una conseguenza sanzionatoria rilevante, e cioè il pagamento di una somma da 20.000 a 120.000 euro (art. 163).

Il Garante per la protezione dei dati personali si è di frequente pronunciato sulle attività di trattamento di dati biometrici, sia in fase di verifica preliminare ex art. 17 del D.Lgs. 196/2003, sia in fase di svolgimento della sua attività ispettiva; ed ha anche pubblicato alcune linee guida relative ad ambiti concettuali affini (si pensi alle Linee guida per il trattamento di dati dei dipendenti privati, Provvedimento 23 novembre 2006, e alle Linee Guida sul rapporto di lavoro pubblico, Provvedimento 10 luglio 2007). Da tale produzione si evince che l'Autorità distingue l'uso dei dati biometrici a fini di autenticazione, e quindi essenzialmente come misura di sicurezza prevista espressamente dalla Regola 2 dell'Allegato B del D.Lgs. 196/2003, da quello a fini di individuazione, cioè come sistema utilizzato per diverse utilità: nel primo caso, accertato il rispetto delle Regole 1-11 dell'Allegato B, l'attività di trattamento dei dati biometrici è stata considerata legittima di per sé; nel secondo caso il trattamento è stato ammesso solo in casi particolari, tenuto conto delle finalità e del contesto in cui sono stati utilizzati dati biometrici (e la verifica preliminare ex art. 17 del D.Lgs. 196/2003 è stata ritenuta essenziale).

In sintesi, la posizione del Garante nei confronti delle nuove applicazioni tecnologiche che sempre più portano all'impiego di informazioni dell'individuo di tipo biometrico è di attento controllo, cercando di allineare le varie esperienze ai principi "tipici" stabiliti dalla legge, anche se in alcune situazioni questo può portare (o porta) ad alcune difficoltà, come nel caso delle firme grafometriche.

4. Le pronunce del Garante per la protezione dei dati personali sui sistemi di firme grafometriche.

Infatti, come si è visto, il testo vigente del Codice dell'Amministrazione Digitale e le nuove regole tecniche in materia di firme elettroniche, emanate con D.P.C.M. 22 febbraio 2013, hanno conferito fondamento giuridico al sistema delle firme grafometriche, sistema che dunque può farsi rientrare tra le firme elettroniche avanzate. Ma è stato già evidenziato il fatto che tale metodo di sottoscrizione elettronica si basa sull'utilizzo di dati grafometrici che hanno natura biometrica, e che quindi implicano l'applicazione della disciplina sulla protezione dei dati personali: nella specie, tra le diverse norme che prevedono l'adempimento di specifici obblighi in capo al titolare, deve essere tenuta in particolare considerazione quella dell'art. 17 del D.Lgs. 196/2003, in cui si stabilisce l'obbligo di verifica preliminare da parte del Garante per i trattamenti che presentano "rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare". Si tenga presente che l'analisi dell'Autorità nell'ambito del c.d. "*prior checking*" non si limita unicamente alla modalità di trattamento dei dati personali nel sistema oggetto di verifica, ma si estende all'opportunità stessa dell'adozione dello specifico sistema biometrico: situazione che si viene a creare quando viene valutata, rispetto al sistema sottoposto all'esame, la corretta applicazione dei principi di necessità, proporzionalità, pertinenza e non eccedenza. Con riferimento al caso di specie tale valutazione potrebbe sollevare un problema di coordinamento tra diverse discipline normative: si potrebbe cioè creare l'anomala situazione in cui il Garante ritenga non corretto un particolare trattamento di dati biometrici di un sistema di firme grafometriche perché ritenuto non necessario per principio, o comunque eccedente la finalità dichiarata, addirittura a prescindere dalla valutazione stessa delle modalità con cui vengono utilizzate le informazioni personali coinvolte. Modalità che potrebbero essere ritenute adeguate dal punto di vista degli obblighi relativi alle misure di sicurezza, o di quelli nei confronti dell'interessato (informativa e raccolta del consenso), ma poi ricevere una verifica preliminare con esito negativo perché viene ritenuto che lo stesso risultato si potrebbe ottenere con metodologie di firma tradizionali. E questo a prescindere dall'esistenza di altre regolamentazioni giuridiche di settore, come quelle del Codice dell'Amministrazione Digitale.

Per comprendere quanto alto sia il rischio del realizzarsi di tale anomalia si deve analizzare la produzione del Garante in sede di verifica preliminare ex art. 17 di sistemi di firma grafometrica: ricordando le due diverse finalità di utilizzo di tali sistemi di sottoscrizione, da una parte quella di autenticazione/identificazione, dall'altra quella di imputazione/dichiarativa. Nel primo caso il Garante, con provvedimento 31 gennaio 2013 su richiesta di Unicredit, ha ammesso il trattamento dei dati biometrici connesso all'uso della metodologia di firma grafometrica, ma legandolo alla specifica fattispecie esaminata ("... a condizione che esso avvenga per le sole finalità dichiarate, con le modalità indicate in narrativa e nel doveroso rispetto di quanto dichiarato dall'istante ai sensi dell'art. 168 del Codice"); e ad una soluzione simile è giunto anche nel recente provvedimento del 23 gennaio 2014 su richiesta di Telecom Italia Trust Technologies s.r.l. e Banca Generali S.p.A., in cui è entrato maggiormente nelle specifiche della fattispecie sottoposta a verifica, con riferimento alla titolarità del trattamento posto in essere nel sistema di firma grafometrica, all'informativa

e al consenso da predisporre per gli interessati (evidenziando la necessità di lasciare in ogni caso la possibilità di usare anche modalità di sottoscrizione “tradizionale” su moduli cartacei), alla conservazione dei dati biometrici di questi ultimi. Per entrambe le situazioni l’Autorità ha poi richiesto l’adozione di “particolari cautele a difesa dei dati biometrici degli utenti, anche in considerazione del fatto che parte del trattamento avverrà attraverso strumenti, tablet, che possono essere utilizzati in mobilità” (nella specie cautele che si concretizzerebbero nella protezione degli apparati utilizzati in modo di impedire che possano essere installati software non autorizzati o che vengano infettati da virus informatici, e predisponendo la possibilità del c.d. “*remote wiping*”, cioè la possibilità di cancellare da remoto il contenuto del tablet nel caso in cui venga manomesso, smarrito o rubato).

Nella seconda ipotesi di utilizzo, in cui lo strumento grafometrico è usato per l’imputazione della dichiarazione elettronica, si registra al momento una sola decisione, quella del 12 settembre 2013 su richiesta di Fineco, che ha autorizzato il sistema ritenendo che questo trattamento dei dati biometrici non risulti connotato da specifici ed evidenti rischi per gli interessati, sempre se effettuato con le misure di sicurezza previste dalla legge; che l’utilizzo della soluzione proposta può contribuire a conferire maggiore certezza nei rapporti giuridici intercorrenti con gli utenti (in particolare dove è richiesta la forma scritta *ad substantiam*); che la firma grafometrica “asseconda legittime esigenze organizzative della società”; che comunque dovranno essere rispettati i diversi obblighi stabiliti dalla legge (ad es. per notificazione, informativa, consenso, misure di sicurezza,...).

Dall’analisi delle pronunce fin qui pubblicate dall’Autorità non si evidenzia quindi il contrasto di cui si è parlato: non ultimo perché in tutti e tre i casi la verifica è stata positiva. E a breve il Garante pubblicherà un provvedimento generale sul trattamento dei dati biometrici che probabilmente affronterà anche le problematiche delle firme grafometriche. Ma certamente anche la semplice possibilità che si crei il conflitto tra le due discipline richiamate deve portare gli operatori del settore, e i futuri utenti della tecnologia delle firme grafometriche, a prestare una maggiore ponderatezza circa gli aspetti di protezione dei dati personali dei soggetti firmatari coinvolti nei vari sistemi grafometrici.

D’altro canto si auspica che anche il Garante per la protezione dei dati personali, in sede di verifica preliminare ex art. 17 del D.Lgs. 196/2003, oppure nell’ambito del provvedimento generale di prossima pubblicazione, presterà attenzione soprattutto alle modalità di trattamento dei dati personali nelle differenti tipologie di firma grafometrica, e non tanto all’opportunità del sistema in sé. Tranne comunque sottoporre ad un’ulteriore riflessione ed approfondimento proprio la modalità di valutazione dei principi di necessità, proporzionalità, pertinenza e non eccedenza rispetto a questo specifico ambito di trattamento dei dati biometrici, che si ritiene debba avvenire in maniera evolutiva e non necessariamente in contrasto con il sempre maggiore sviluppo dell’innovazione tecnologica.

PUNTI FERMI E CRITICITÀ NELLA DISCIPLINA DEL COMMERCIO ELETTRONICO A 10 ANNI DAL RECEPIMENTO DELLA DIRETTIVA UE 31/2000

Leonardo Bugiolacchi

 *Multimedia*



Clicca sull'immagine o fotografa il QrCode
per accedere al MediaBook CLIOedu

Sommario: 1. Premessa. – 2. I “punti fermi”. 2.1. I recenti interventi a sostegno del commercio elettronico; 2.2. La conclusione dei contratti del commercio elettronico; 2.3. La “non autosufficienza” della disciplina di cui al d.lgs. n. 70/2003. – 3. Le “criticità”. Note in tema di responsabilità dell’*host provider*.

1. Premessa

È noto che il commercio elettronico rappresenta uno dei settori di maggiore utilizzazione delle tecnologie dell’informazione e della comunicazione e, più in generale, una delle aree più rilevanti della società dell’informazione¹.

Grazie a tali tecnologie è stato – ed è – possibile affiancare ai mercati tradizionali (fisici) nuovi ambienti di scambio di beni e servizi; in questo modo al mercato inteso in senso fisico si è venuto ad aggiungere un luogo virtuale, un marketplace elettronico, al quale si accede per mezzo delle nuove tecnologie, tanto che il commercio elettronico è divenuto uno dei fenomeni caratterizzanti la c.d. “società dell’accesso”, come la definita in un noto scritto Jeremy Rifkin².

In questo quadro l’accesso all’ambiente interconnesso, realizzato dal web diviene preconditione della fruizione di beni e servizi, che vengono acquisiti con modalità innovative, dall’altro, molto spesso, rappresenta modalità stessa di fruizione dei servizi richiesti, come accade, ad esempio, mediante il downloading di software.

Il legislatore europeo ha quindi individuato, a partire dalla metà degli anni novanta del secolo scorso, nello sviluppo del commercio elettronico (che, dal punto di vista della sua qualificazione normativa costituisce un “servizio della società dell’informazione³) una grande opportunità per l’occupazione nella Comunità, in particolare per quanto riguarda le piccole e medie imprese⁴.

Ci è quindi sembrato ineludibile svolgere, a dieci anni dall’entrata in vigore del decreto 70/2003, di recepimento della direttiva 31 del 2000, un sintetico bilancio dello “stato dell’arte” in materia, evidenziando, come risulta dal titolo del mio intervento, i “punti fermi”, vale a dire le consolidazioni ormai affermatesi rispetto a talune questioni in passato oggetto di dibattito, e le “criticità” della disciplina, vale a dire i temi rispetto ai quali, presso giurisprudenza e dottrina, persistono incertezze interpretative e qualche lacuna normativa, in una visuale, tengo a precisare, esclusivamente civilistica.

¹ **Il presente scritto, con talune integrazioni e con l’aggiunta dell’apparato di note, rappresenta la trascrizione dell’intervento effettuato in occasione del Convegno ANDIG svoltosi in Roma il 29 ottobre 2013.* 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 in essa possiedono le tecnologie dell’informazione e della comunicazione, sia grazie all’avvento della telematica che al processo di liberalizzazione che ha interessato il settore tele comunicativo. Tale locuzione si rinviene per la prima volta nel c.d. “Rapporto Delors” del 1993, nel quale la società dell’informazione è considerata una dimensione nuova ed essenziale per il rilancio dell’economia europea ed è stata poi ripresa nel 1994, nel c.d. “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. Sulla categoria dei contratti di accesso, quale giuridicizzazione dei rapporti propedeutici all’acquisto di beni o servizi on line, si veda in dottrina PALIMIEMI, *I contratti di accesso*, Milano, 2000.

³ Cfr., al riguardo, l’art. 1, comma, 1, d.lgs. n. 70 del 2003, di recepimento della direttiva 2000/31.

⁴ Si veda, in proposito, il considerando n. 2 della direttiva 2000/31.

2.I “punti fermi”

Prendiamo quindi le mosse da quelli che ho inteso qualificare i “punti fermi”, vale a dire, appunto, le consolidazioni a 10 anni dal recepimento appena menzionato, premettendo come alla grande attenzione degli organi europei verso il nuovo *marketplace* elettronico ed all’ampiezza del dibattito sul rapporto tra diritto e tecnologia che ad essa si è accompagnata⁵, non abbia inizialmente corrisposto, soprattutto nel nostro paese, un sostanziale sviluppo dell’e-commerce.

2.1. I recenti interventi a sostegno del commercio elettronico.

Di recente, però, è tornata in primo piano la centralità del commercio elettronico quale strumento di rilancio dell’intero mercato interno europeo, come risulta da una serie di documenti⁶.

Il primo di essi può essere individuato nella comunicazione della Commissione del 19 maggio 2010, intitolata “Un’agenda digitale europea”, la quale stabilisce la strategia della commissione diretta, soprattutto, a semplificare le transazioni *on line* ed creare un mercato digitale unico basato su internet veloce e superveloce e su applicazioni interoperabili. Tra le specifiche aree d’azione dell’agenda digitale vi è quella incentrata sul lancio di una strategia europea per il miglioramento dei sistemi alternativi di risoluzione delle controversie.

Vi è poi la Risoluzione del Parlamento europeo del 21 settembre 2010 sul completamento del mercato interno per il commercio elettronico, la quale: evidenzia il ruolo di quest’ultimo per il rilancio “sostenibile” del mercato interno; sottolinea altresì come il settore dell’e-commerce sia tra quelli che racchiudono le maggiori potenzialità di crescita e di occupazione future; rileva come il commercio elettronico rappresenti una forza vitale di internet ed un mercato chiave per l’Unione europea nel XXI secolo, potenzialmente in grado di rimodellare il mercato interno europeo e di contribuire all’economia della conoscenza nel contesto della strategia EU 2020, anche grazie allo sviluppo e alla promozione di nuove forme di imprenditorialità per le piccole e medie imprese.

Successivamente, nel gennaio 2012, è stato approvato un piano d’azione per l’e-commerce 2012-

⁵ È noto infatti il dibattito relativo al fatto se l’emersione di nuove modalità di svolgimento di rapporti giuridici tradizionali (si pensi, ad esempio, alla possibilità che l’incontro di volontà, ossia l’accordo, in cui si sostanzia il contratto, avvenga non solo a distanza, ma con uno scambio di e-mail, oppure con la semplice digitoppressione di un tasto del proprio computer – c.d. modalità di conclusione del contratto “point and click”, oppure al fatto che il pagamento della merce o del servizio avvenga con moneta cosiddetta “elettronica”) imponesse l’adozione di nuove regole giuridiche, oppure se quelle già esistenti potessero ben adattarsi anche a regolare i nuovi fenomeni generati dalle tecnologie digitali. Per tali problematiche può leggersi PASCUZZI, *Il diritto dell’era digitale*, Bologna, 2002: 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, 105 e ss.

⁶ Su tale recupero di centralità del commercio elettronico presso gli organi comunitari, sia consentito il rinvio a BUGIOLACCHI, *Commercio elettronico e odr (online dispute resolutions) dopo il Regolamento n. 524/2013 dell’Unione europea*. Gli strumenti alternativi di risoluzione delle controversie dei consumatori, in *Resp.civ. prev.*, 2013, 1403 e ss.

2015, nella prospettiva della accelerazione dello sviluppo dei servizi on line ed avente lo scopo di raddoppiare, entro il 2015, la quota del commercio elettronico nell'ambito delle vendite al dettaglio (pari al 3,4% al momento dell'adozione del piano) e quella della economia di internet in relazione al PIL europeo⁷.

Questa nuova fase di impulso all'ulteriore sviluppo del commercio elettronico sta quindi avvenendo all'interno del quadro giuridico di riferimento rappresentato dalla già citata direttiva 2000/31, e, per il nostro paese, dal d. lgs. n. 70 del 2003 di recepimento, non avendo gli organi europei ritenuto necessaria né opportuna una revisione della direttiva stessa, considerata equilibrata, e ciò sebbene sia emersa l'esigenza di chiarire l'interpretazione di alcune sue parti al fine di migliorarne l'efficacia applicativa, specialmente per quanto attiene, in tema di responsabilità dei cc.dd. "prestatori intermediari", il concetto di consapevolezza dell'illecito ("*actual knowledge*", fondamentale per stabilire l'eventuale esenzione da responsabilità anche alla luce del sempre più frequente coinvolgimento di quella particolare categoria di provider che rappresentano sconfinata piattaforme digitali, dai motori di ricerca ai "contenitori di contenuti" quali Youtube) e di precisazione delle condizioni di esonero da responsabilità, soprattutto del provider di hosting, ma sul punto si tornerà più avanti⁸.

Ancora, il 21 maggio 2013 è stato emanato il Regolamento europeo n. 524 del 2013, relativo alla risoluzione delle controversie online dei consumatori, il quale pure ribadisce l'importanza anche mediante la maggior diffusione e facilità di accesso a meccanismi di adr, di accrescere la fiducia dei consumatori nei confronti di questo mercato⁹.

In ambito nazionale giova ricordare che il 1° marzo 2012, con DM sviluppo economico è stata istituita l'agenda digitale italiana (ADI) la quale ha, al suo interno, un organo operativo, denominato "cabina di regia", strutturato in 6 gruppi di lavoro, corrispondenti a sei assi considerati strategici, uno di questi dedicato proprio all'e-commerce.

Risulta quindi inevitabilmente, che il generale obiettivo di rilancio dell'e-commerce possa ben essere perseguito, nell'idea degli organi europei, senza intervenire sulla direttiva risalente ad ormai

⁷ Tale piano prevede, per la realizzazione degli obiettivi in esso contenuti, una serie di azioni, consistenti soprattutto: nella piena applicazione della direttiva sul commercio elettronico; nella definizione di una strategia europea per la protezione intellettuale; nel contrasto alle pratiche commerciali scorrette (sulle quali si segnalano recenti interventi della nostro Garante per la concorrenza ed il mercato, adottati ai sensi dell'art. 20 e ss. Cod. consumo, con i quali è stato inibito, per la prima volta, l'accesso a siti internet che adottavano pratiche commerciali scorrette); nella migliore informazione e formazione degli operatori; nella maggior protezione dei consumatori; nell'efficienza del sistema dei pagamenti e delle consegne; nella efficacia nella risoluzione delle controversie.

⁸ Su questi argomenti sia consentito il rinvio a 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.

⁹ D'altronde, quasi tutti i documenti citati nel testo prevedono, tra gli strumenti finalizzati ad accrescere la fiducia dei consumatori nel nuovo mercato, l'utilizzazione di piattaforme online per la risoluzione alternativa delle controversie (RAC), soprattutto mediante la creazione di organismi centralizzati di gestione delle controversie da risolvere con procedure di ODR (online dispute resolutions), tanto è vero che a tale proposito la già menzionata Risoluzione del Parlamento europeo del settembre 2010 parla di istituzione di un "sistema di informazione europeo per il consumatore elettronico". Ancora più specificamente, nella comunicazione della Commissione del 13 aprile 2011, intitolata "L'atto per il mercato unico – Dodici leve per stimolare la crescita e rafforzare la fiducia – Insieme per la crescita", la Commissione medesima ha collocato la legislazione in materia di risoluzione alternativa delle controversie (ADR), includendo anche la materia del commercio elettronico, nel novero delle dodici leve per stimolare la crescita e rafforzare la fiducia nel mercato unico.

13 anni fa, in quanto considerata tuttora sufficientemente bilanciata, seppur con qualche distinguo, sul quale com detto mi soffermerà nel prosieguo, in tema di regime di responsabilità degli internet provider, soprattutto di hosting.

2.2. La conclusione dei contratti del commercio elettronico.

La disciplina contenuta nel d.lgs. n. 70/2003 di recepimento della direttiva europea, per quanto attiene alle modalità di conclusione telematica del contratto ed al regime informativo precontrattuale (peraltro applicabile principalmente ai contratti conclusi con il procedimento point and click, visto che per i contratti nei quali la sequenza proposta-accettazione avviene mediante mail, il decreto non trova applicazione per sua stessa, espressa previsione) non ha posto particolari problemi interpretativi.

E' noto, d'altronde, come il legislatore comunitario, sebbene in una prima fase avesse immaginato di armonizzare tra gli stati membri le disposizioni sui meccanismi di perfezionamento dei contratti conclusi per via elettronica, pur se relativamente al solo ambito dell'e-commerce, abbia poi abbandonato tale strada, preferendo limitarsi all'introduzione di talune disposizioni di garanzia per il destinatario dei servizi della società dell'informazione¹⁰. Ciò emerge chiaramente dal principio generale, recepito nel nostro ordinamento dall'art. 13, primo comma, d.lgs. n. 70/2003, in base al quale le norme sulla conclusione dei contratti si applicano anche nel caso di contrattazione on line.

Nonostante qualche disputa dottrinaia avente ad oggetto la rilevanza o meno dell'obbligo di accusare ricevuta dell'inoltro dell'ordine all'interno del procedimento di formazione del contratto, la conclusione con il mezzo telematico è stata pacificamente accolta come pienamente legittima anche in virtù del principio della tendenziale libertà delle forme tipica del nostro diritto privato e non quindi non ha destato particolari problemi applicativi (e ciò anche grazie alla già citata previsione, contenuta nella direttiva e recepita nell'art. 13 del d.lgs. n. 70 del 2003, secondo cui le norme sulla conclusione del contratto si applicano anche nei casi in cui il destinatario del servizio inoltri il proprio ordine per via telematica, in linea con quella più generale della direttiva che, nel suo considerando n. 34 afferma che gli stati membri non possano prevedere una legislazione interna che ostacolasse la conclusione telematica dei contratti e, all'art. 9, prevede che gli stati membri provvedano affinché i loro ordinamenti rendano possibili contratti per via elettronica, a causa della assenza di un regime armonizzato in materia contrattuale a livello europeo).

Il dibattito cui si è fatto cenno scaturisce dalla previsione, introdotta dal secondo comma dell'art. 13, d.lgs. n. 70/2003, dell'obbligo del prestatore del servizio di inviare una ricevuta al destinatario del servizio, senza ingiustificato ritardo ed in via telematica, dell'inoltro dell'ordine, contenente anche il riepilogo delle condizioni di contratto. La maggior parte della dottrina ritiene che non

¹⁰ In argomento si veda, diffusamente, BRAVO, voce "Commercio elettronico", in Enc. Dir., agg. , 2012, 292. In particolare, la prima proposta di direttiva conteneva, all'art. 11, la previsione secondo la quale il contratto si sarebbe dovuto considerare concluso quando il destinatario avesse ricevuto dal prestatore, per via elettronica, la ricevuta di ritorno dell'accettazione del destinatario medesimo.

si sia in presenza di un obbligo che influisce sul procedimento di formazione del contratto, già conclusosi al momento dell'inoltro dell'ordine, da intendersi come accettazione della proposta, rappresentata dall'offerta al pubblico presente sul sito web di e-commerce¹¹.

Si tratterebbe quindi soltanto di una ulteriore procedimentalizzazione del rapporto che però non pare in grado di incidere sul momento perfezionativo del contratto, ma avente piuttosto la funzione di soddisfare esigenze di certezza dei rapporti intercorsi, nonché di fornire al destinatario del servizio il supporto probatorio per far valere il proprio diritto in caso di necessità, sempre nella citata prospettiva della *ratio* di accrescimento della fiducia del consumatore (e del contraente in genere) verso il nuovo mercato elettronico.

Sul punto giova solo ricordare come in dottrina si sia giustamente evidenziato che nel commercio elettronico non è comunque individuabile – come peraltro anche nella realtà off line – un unico modello di incontro delle volontà, in quanto, a seconda del contenuto del sito web, le informazioni in esso presenti possono anche essere valutate come invito a proporre, nel quale caso, la ricevuta di “inoltro dell'ordine” potrebbe anche assolvere alla funzione di manifestare l'accettazione da parte del prestatore del servizio; è ovvio che una tale impostazione insista poi sulla necessità di verificare, caso per caso, quale sia la natura giuridica delle dichiarazioni negoziali in base ai contenuti presenti sul sito¹².

Qualche contrasto interpretativo, confermato anche da comunque esigui interventi giurisprudenziali, attiene alla idoneità o meno del *click* sul *form* di accettazione, al fine di soddisfare il requisito della approvazione specifica per iscritto della clausola vessatoria ai sensi dell'art. 1341, secondo comma, c.c. Se infatti non sussistono dubbi sul fatto che, proprio in virtù del principio di libertà delle forme, la tecnica del *point and click* (o tasto virtuale) sia sufficiente a manifestare validamente il consenso contrattuale, così perfezionando il contratto (ovviamente laddove per il singolo contratto non sia prevista la forma scritta *ad substantiam*), diversa è la questione nel caso in cui il contratto – solitamente predisposto dal prestatore del servizio – presenti delle clausole vessatorie ai sensi e per gli effetti dell'art. 1341, secondo comma, c.c.¹³ In tale ambito si assiste a interpretazioni elastiche¹⁴, di segno positivo, ad altre, maggiormente rigorose, le quali ritengono che la validità della clausola sia subordinata alla sua specifica sottoscrizione con firma digitale (più correttamente si dovrebbe parlare ora di firma elettronica avanzata, qualificata o digitale, secondo la terminologia contenuta nel vigente Codice dell'Amministrazione digitale), in considerazione del fatto che lo specifico riferimento alla sottoscrizione, risultante dal secondo comma dell'art. 1341 c.c., postulerebbe la formale individuazione soggettiva del dichiarante e non una “mera” manifestazione di volontà¹⁵.

¹¹ In tal senso si veda, ad esempio, La conclusione dei contratti telematici nel diritto privato europeo, in *Contr.*, 201, spec. 308; PENNASILICO, La conclusione dei contratti on line tra continuità e innovazione, in *Dir. inf.*, 2004, 825.

¹² In questo senso si veda BRAVO, voce “Commercio elettronico”, cit., spec. 293 e ss.

¹³ D'altronde che anche i “formulari” dei contratti on line possano contenere clausole operative, così da rendere operativa la regola di cui all'art. 1341, secondo comma, è un dato scontato, come ha avuto modo di precisare la stessa Cassazione (Cass. civ., 22 marzo 2006, n. 6312, inedita), laddove ha affermato come “condizioni generali di contratto unilateralmente predisposte e contrattazione mediante moduli o formulari appaiono concetti non solo indifferenti quanto al mezzo tecnico di veicolazione – stampato o formato elettronico – ma anche fattori destinati a subire un perfezionamento attraverso le tecnologie digitali e del web”.

¹⁴ È questa la posizione del Giudice di pace di Partanna, 1° febbraio 2002, in *Contr.*, 2002, 869, secondo il quale la sottoscrizione di una clausola vessatoria ben può avvenire con la digitazione sul tasto negoziale “accetto” riferentesi alla clausola.

¹⁵ In tal senso, di recente, Trib. Catanzaro, 30 aprile 2012 (ord.), in *Resp. civ. prev.*, 2013, 2015.

2.3. La “non autosufficienza” della disciplina di cui al d.lgs.n. 70/2003.

Un'altra riflessione incontrovertibile riguarda il fatto che la disciplina del d. lgs. n. 70 del 2003, in quanto relativa non solo ai contratti b to c ma anche a quelli b to b (si parla, non casualmente, di prestatori e destinatari del servizio e non di “professionisti” e “consumatori”), come era apparso fin dall'inizio non è “autosufficiente”, ma necessita di essere integrata, nei casi in cui una delle parti del rapporto sia un consumatore, dalla normativa complessiva - generale e speciale, cioè dedicata sia alle regole generali, applicabili a tutti i contratti di consumo, sia quelle appunto speciali, in quanto riferite a specifiche attività, penso ai servizi finanziari a distanza, ai pacchetti turistici, etc.) contenuta nel codice del consumo.

Il che vuol dire che, a seconda dell'oggetto del bene o servizio scambiato, ove una delle parti sia un consumatore, troverà necessaria applicazione anche la disciplina di protezione del consumatore, con la conseguenza che l'operatore del diritto sarà chiamato – per ogni tipologia di contratto di consumo – a ricostruire la disciplina complessiva utilizzando i segmenti normativi presenti non solo nel d.lgs. n. 70 del 2003, ma anche nel Codice del consumo.

Sotto tale profilo di interazione tra disciplina consumeristica di carattere generale ed attività di e-commerce si segnalano due abbastanza recenti interventi dell'autorità garante della concorrenza e del mercato (fine 2012), che ha inibito l'accesso a due siti di e-commerce in quanto effettuavano pratiche commerciali scorrette, fondando il proprio potere di intervento sull'art. 27, III comma, cod. consumo (che consente all'autorità la sospensione provvisoria delle pratiche) e sugli artt. 14, 15 e 16 del d.70 del 2003 i quali, nei loro ultimi comma, prevedono come l'autorità amministrativa di vigilanza possa esigere, anche d'urgenza, dal provider di porre fine alle violazioni commesse sui siti rispetto ai quali egli svolge un ruolo meramente tecnico; con i medesimi provvedimenti sono state comminate ai titolari dei siti anche pesanti sanzioni pecuniarie, sempre secondo quanto previsto dal Codice del consumo.

Ulteriore conferma della necessaria, continua e costante integrazione tra d. lgs. n. 70 del 2003 e normativa consumeristica è data dal contenuto della recente direttiva n. 83 del 2011 in tema di tutela dei diritti dei consumatori¹⁶, di prossimo recepimento nel nostro diritto interno la quale, tanto per fare un esempio, in tema di esercizio del diritto di recesso nei contratti a distanza, stabilisce, all'art. 11 che il professionista possa offrire al consumatore la possibilità di compilare e inviare elettronicamente il modulo di recesso riportato in un allegato alla direttiva e che, in tal caso, il professionista comunichi “senza indugio” al consumatore una conferma di recepimento del recesso su un supporto durevole.

Infine, ed ancora nella prospettiva della non autosufficienza normativa del d.lgs. n. 70 del 2003 non può non darsi conto della recente proposta di Regolamento per un “Diritto comune europeo della vendita”¹⁷, la quale, nella prospettiva del legislatore europeo, dovrebbe porsi come strumento

¹⁶ Trattasi di direttiva che abroga le precedenti direttive 85/577 sui contratti negoziati fuori dei locali commerciali e 97/7 sulla protezione dei consumatori nei contratti a distanza, oltre che modificativa della storica direttiva generale 93/13.

¹⁷ Su tale interessante intervento comunitario si veda, in dottrina, D'AMICO, Direttiva sui diritti dei consumatori

“opzionale” (opt-in), vale a dire di carattere facoltativo, alternativo alle regole che, secondo i vari meccanismi interni di diritto internazionale privato, dovrebbero disciplinare i rapporti contrattuali transfrontalieri. Tale disciplina, il cui ambito applicativo riguarda – sia pur con significative differenze – i rapporti tra imprese e consumatori e quelli tra imprese, alla condizione che almeno una di esse sia una “piccola impresa” secondo i requisiti previsti nella disciplina, è in grado di produrre i suoi effetti anche sul commercio elettronico.

Questa proposta normativa, infatti, prende atto della fase avanzata di sviluppo del commercio elettronico e ne trae le dovute conseguenze in tema di individuazione delle regole sulla formazione del contratto. In proposito, un’intera sezione del testo, è dedicata ai “contratti conclusi con mezzi elettronici” e in essa, all’art. 24, sono stabiliti obblighi analoghi a quelli previsti dalla disciplina sul commercio elettronico vigente per quanto attiene alle informazioni ed agli altri obblighi precedenti alla conclusione del contratto, che vengono qui però maggiormente precisati, proprio in considerazione della diverse realtà concrete nelle quali può atteggiarsi l’offerta di beni o servizi *on line*, mentre negli artt. 30 e seguenti è contenuta la disciplina relativa alla “conclusione del contratto”, i quali non recano particolari differenze rispetto alla struttura del contratto quale accordo, così come previsto dal nostro codice civile, né rispetto ai meccanismi perfezionativi, eccezion fatta, forse, per l’individuazione degli elementi idonei ad attribuire al contenuto di un sito il carattere di una offerta al pubblico, tale da rendere possibile un modello di perfezionamento del contratto analogo a quello contemplato dal nostro articolo 1336 c.c.¹⁸.

3. Le “criticità”. Note in tema di responsabilità dell’host provider

I profili critici della disciplina contenuta nella normativa di recepimento della direttiva 31/2000 riguardano a mio, avviso, come già accennato, la necessità di meglio definire le condizioni di responsabilità del provider, con particolare riferimento al fornitore di hosting.

Si tratta, peraltro, di un tema caro al sottoscritto ed al quale ho dedicato la maggior parte delle mie ricerche in tema di diritto delle nuove tecnologie.

In primo luogo, sul punto ritengo che non sia più possibile eludere il disaccordo esistente tra l’interpretazione giurisprudenziale consolidatasi sull’art. 16, primo comma, lett. b) d.lgs. 70 del 2003, secondo cui il provider incorrerebbe in responsabilità ogni qual volta ometta di rimuovere un contenuto illecito del quale sia stato reso consapevole a seguito della comunicazione di qualsiasi terzo¹⁹ (solitamente la vittima dell’illecito) e la lettera della norma, la quale a mio avviso introduce,

e Regolamento sul Diritto comune europeo della vendita: quale strategia dell’Unione europea in materia di armonizzazione?, in *Contr.*, 2012, 611; STANZIONE, Il regolamento di Diritto comune europeo sulla vendita, *ivi*, 624.

¹⁸ In questo senso si veda BRAVO, voce “Commercio elettronico”, *cit.*, 296.

¹⁹ In questo senso, in giurisprudenza, Trib. Catania, 29 giugno 2004, in *Resp. civ. prev.*, 2005, 188; Trib. Bari, 13 giugno 2006, in *Dir. Internet*, 2006, 563; Trib. Trani, 14 ottobre 2008, in *Danno e resp.*, 2009, 1059; Trib. Roma, 22 gennaio 2010, *inedita*. Tutte queste decisioni si basano sul presupposto (talvolta implicitamente) dell’autonomia precettiva tra

rispetto al più generico testo dell'art. 14 direttiva, una nozione di conoscenza "qualificata" dell'illecito quale presupposto dell'obbligo di intervento di rimozione del materiale illecito (questo grazie alla presenza dell'inciso, "su comunicazione delle autorità competenti")²⁰.

Proprio in virtù di tale introduzione di una conoscenza qualificata, non sarebbe possibile, ad avviso di chi scrive, ipotizzare un obbligo di rimozione, il cui inadempimento farebbe sorgere la responsabilità dell'host provider, prima ancora che questi abbia ricevuto al riguardo una comunicazione da parte delle autorità competenti.

Una tale impostazione, che non è possibile approfondire in questa sede, oltre che maggiormente rispettosa del testo e della struttura dell'art. 16, che pare a ben vedere costruita su una responsabilità del provider fondata su una lettura combinata e coordinata delle lettere a) e b) che compongono il suo primo comma, sembra anche in grado di rendere ragione del contenuto di un'altra disposizione del d.lgs. n. 70 del 2003, anch'essa di portata innovativa rispetto al testo della direttiva, vale a dire quella contenuta nel terzo comma dell'art. 17, secondo la quale il provider è responsabile civilmente qualora disattenda l'obbligo di informare le autorità competenti quando abbia avuto conoscenza del carattere illecito o pregiudizievole per un terzo del contenuto di un servizio al quale assicura l'accesso.

Ebbene, la previsione di tale ulteriore fattispecie "tipica" di responsabilità del provider, ben si spiega proprio con l'introduzione della nozione di conoscenza "qualificata", ora richiesta dall'art. 16, tanto è vero che il sistema risultante dal combinato disposto degli artt. 16 e 17 d.lgs.n. 70 del 2003 così può essere ricostruito: a) l'host provider non è custode dei contenuti presenti sui siti (o contenitori in genere) dei quali rende possibile il funzionamento e aggiornamento continui (stante il principio generale dell'assenza di un obbligo di sorveglianza, ai sensi del primo comma dell'art. 17 d.lgs. n. 70 del 2003) e, come tale, non può mai risponderne, ove ne sia a conoscenza (vedi art. 17, primo comma e art. 16, lett. a); b) nel caso in cui l'host provider abbia conoscenza dell'illecito, ad opera di un soggetto non qualificato, dovrà informare di ciò le autorità competenti (art. 17, comma terzo); c) saranno poi queste ultime, nei casi in cui l'illiceità sia manifesta, ad effettuare al provider la comunicazione di cui alla lettera b) dell'art. 16, dalla quale soltanto può derivare l'obbligo di rimozione immediata²¹.

Ugualmente non procrastinabile è la posizione di regole più chiare e maggiormente armonizzate in tema di *notice and take down*, vale a dire che necessitano di essere stabiliti modi e tempi dell'intervento

le lettere a) e b) dell'art. 16 del d.lgs. n. 70 del 2003, nel senso che il provider di hosting risponderrebbe: 1) per il fatto di essere venuto a conoscenza di attività o informazioni illecite sui siti gestiti, in base al disposto della lettera a); 2) per il fatto di non aver adempiuto all'obbligo di tempestiva rimozione dopo la segnalazione delle autorità competenti, con condotta che, anche ad avviso di parte della dottrina, sconfinerebbe nel dolo.

²⁰ Anche se, a ben vedere, di recente alcune pronunce (Trib. Firenze, 25 maggio 2012, in *Corr. Giur.*, 2013, 505; Trib. Roma, 20 ottobre 2011, inedita) hanno – più o meno espressamente – collegato la responsabilità dell'host provider alla mancata rimozione dei contenuti nonostante la comunicazione delle autorità competenti, manifestando adesione alla interpretazione fornita sopra, nel testo.

²¹ Per tale ricostruzione si rinvia a BUGIOLACCHI, *La responsabilità dell'host provider alla luce del d.lgs. n. 70/2003: esegesi di una disciplina dimezzata*, in *Resp. civ. prev.*, 2005, 188 e ss. Nel medesimo senso, in dottrina, RICCIO, *La responsabilità degli internet providers nel d.lgs. n. 70/2003*, in *Danno e resp.*, 2003, 1158; COMANDE', *Al via l'attuazione della direttiva sul commercio elettronico, ma ... serve un maggior coordinamento*, *ivi*, 2003, 812; CASAROSA, *Wikipedia: esonero dalla responsabilità*, *ivi*, 2009, 149; TRUCCO, *Pubblicazione d'immagini personali in rete e responsabilità del provider*, in *Dir. internet*, 2006, 565.

di rimozione da parte dell'host provider, sia nel caso in cui si ritenga che egli sia tenuto ad attivarsi anche a prescindere da una comunicazione delle autorità competenti, sia che invece il cui obbligo si consideri subordinato appunto ad una conoscenza "qualificata". Trattasi di questione che, peraltro, aveva suscitato fin dall'inizio critiche alla direttiva 2000/31, che nulla aveva previsto sul punto e che condotto taluni stati membri, in sede di recepimento, ad introdurre meccanismi proceduralizzati di *notice and take down* che coinvolgono solitamente autorità di vigilanza, come avvenuto ad esempio in Portogallo.

Ho parlato in precedenza di ineludibilità della soluzioni di tali questioni in quanto la tematica della responsabilità degli hosting provider, dopo aver suscitato un interesse notevolissimo dopo l'emanazione del d. 70 aveva conosciuto invece poi una sorta di oblio, probabilmente in considerazione della quasi totale assenza di un diritto giurisprudenziale sul punto.

Negli ultimi anni, invece, soprattutto in conseguenza dello sviluppo delle grandi piattaforme digitali, sconfinati contenitori/aggregatori di contenuti immessi dagli stessi utenti (per questo UGC), che funzionano e assumono valore aggiunto solo grazie ai sistemi di categorizzazione, indicizzazione e ricerca – anche agevolata - dei contenuti, la responsabilità dei provider è ridivenuta di scottante attualità, anche sulla scorta di casi di forte impatto mediatico, che hanno visto coinvolti i maggiori soggetti operanti nel settore (si pensi a Google, o a Youtube).

Ebbene, tali servizi forniti dai provider (i quali finiscono così in qualche modo per assommare le qualità degli host provider a quelle dei motori di ricerca tout court), in aggiunta a quelli di semplice messa a disposizione della memoria, hanno da un lato reso più agevole la rintracciabilità di materiali illeciti, e dall'altro hanno anche posto la questione della responsabilità di tali prestatori intermediari, i quali eccederebbero il ruolo meramente tecnico (automatico e passivo) al quale il legislatore europeo aveva inteso collegare il loro esonero da responsabilità per i contenuti veicolati e, soprattutto, danno luogo ad attività di hosting forse non immaginabili al momento della redazione della direttiva (sono noti al riguardo i casi Google- Vividown, come quelli che hanno riguardato Rti Mediaset e le sue azioni nei confronti di Youtube per la tutela dei propri diritti d'autore e, ancora più di recente, le decisioni giurisprudenziali, anche di carattere contrastante, intervenute in tema di responsabilità del motore di ricerca per la funzione di auto completamento della ricerca, in quanto le locuzioni che il sistema visualizzava in automatico contenevano affermazioni di apparente, immediato contenuto diffamatorio nei confronti dei soggetti rispetto ai quali l'utente stava effettuando una ricerca²².

E' evidente che la descritta centralizzazione di contenuti (dati, immagini, informazioni in senso lato) su enormi piattaforme digitali continuamente alimentate dall'attività di *uploading* degli utenti, ha reso necessaria, da parte dei fornitori di "memoria" tendenzialmente stabile (gli host provider, appunto), l'adozione di tecnologie, tendenzialmente automatiche, di organizzazione dei contenuti, al fine di renderne possibile il reperimento da parte di chi intende raggiungerle.

²² Il c.d. sistema di *autocomplete*, fornito ad esempio da Google. Sul punto, secondo Trib. Pinerolo, 2 maggio 2012, in Resp. civ. prev., 2013, 234, il motore di ricerca non sarebbe responsabile. Al contrario, ad avviso di Trib. Milano, 24 marzo 2011, ivi, 2011, 1320 e Trib. Milano, 25 maggio 2013, ivi, 1996, il motore di ricerca - la cui attività viene considerata riconducibile a quella dell'host provider - sarebbe invece responsabile in quanto non si limiterebbe a fornire passivamente servizi di ospitalità di contenuti altrui, ma svolgerebbe attività ulteriori, non meramente automatiche o passive, perdendo così la posizione di neutralità cui è legata l'esenzione da responsabilità ai sensi degli artt. 15 e 16 d.lgs. n. 70 del 2003.

Un tale mutamento funzionale è stato individuato, come accennato appena sopra, dalla stessa giurisprudenza, la quale ha così elaborato la figura, di creazione giurisprudenziale, dell'host provider "attivo", spesso motivata con richiamo alla giurisprudenza della Corte di Giustizia europea, che ha avuto occasione di affermare il principio secondo cui l'art. 14 della direttiva 2000/31 (disciplinante l'esonero "condizionato" da responsabilità dell'hosting provider o, a seconda delle prospettive, l'individuazione delle fattispecie tipizzare di *fault liability* di tale soggetto) debba essere interpretato nel senso che tale norma trovi applicazione al prestatore di un servizio di posizionamento su internet solo qualora tale prestatore non abbia svolto un ruolo attivo atto a conferirgli la conoscenza o il controllo dei dati memorizzati²³; la stessa giurisprudenza comunitaria ha anche affermato il principio, strettamente connesso a quello appena richiamato, per cui, in base al considerando n. 42) della direttiva 2000/31 risulta che le deroghe alla responsabilità dei prestatori intermediari previste dalla direttiva riguardano esclusivamente i casi in cui l'attività del provider sia di ordine "meramente tecnico, automatico e passivo", nel senso cioè che il prestatore "non conosce né controlla le informazioni trasmesse e memorizzate".

Ebbene, non si può fare a meno di notare come una tale impostazione imponga qualche riflessione critica²⁴.

La prima di esse attiene al fatto che la verifica della natura "attiva" o meramente passiva del fornitore del servizio di memorizzazione non può che essere compiuta in concreto, sulla base di indici che non presentano però aggancio normativo alcuno. Non a caso, infatti, la stessa Corte di Giustizia ha affermato che, per quanto riguarda il servizio di posizionamento offerto dal programma Adwords, dal quale deriva l'ordine di visualizzazione, in funzione, in particolare, del pagamento degli inserzionisti, esso non possa avere come effetto di privare il provider (Google, in quel caso) delle deroghe in materia di responsabilità previste dalla direttiva 2000/31²⁵; allo stesso modo questa decisione ha precisato come il fatto che la parola chiave selezionata e il termine di ricerca inserito da un utente della rete coincidano non sia di per sé sufficiente a ritenere che il provider conosca o controlli i dati inseriti dagli inserzionisti nel suo sistema e memorizzati sul suo server.

Ne risulta quindi un meccanismo di attribuzione della responsabilità che, proprio in quanto basato su un approccio necessariamente casistico, priva la condotta del provider del carattere di prevedibilità circa la eventuale valutazione giudiziale. Ciò tanto più in quanto, come è stato di recente osservato da autorevole dottrina, non si è ancora verificata, in tale ormai nevralgico settore del diritto (nevralgico in quanto sempre più spesso impatta su tematiche ad elevata rilevanza sociale), quella "technical disclosure" indispensabile per rendere comprensibile il rapporto tra attività svolte dal provider e loro incidenza su possibili effetti non meramente automatici sui contenuti²⁶. Si intende con ciò dire che fin quando non si comprende, da un punto di vista tecnico, in che

²³ In tal senso, Corte Giustizia Ce, 23 marzo 2010 e Corte Giustizia, 12 luglio 2011.

²⁴ Per una trattazione più diffusa delle riflessioni che seguono, nel testo, sia consentito il rinvio a BUGIOLACCHI, Evoluzione dei servizi di *hosting provider*, conseguenze sul regime di responsabilità e limiti dell'attuale approccio case by case, in Resp. civ. e prev., 2013, 1997 e ss.

²⁵ Così Corte di Giustizia Ce, 23 marzo 2010, cit.

²⁶ Il riferimento è a SICA, Responsabilità del provider: per una soluzione "equilibrata" del problema, in Corr. Giur., 2013, 505.

modo la predisposizione di software *lato sensu* “gestionali” intervenga sui materiali, risulta anche difficile comprendere se le funzionalità offerte dai provider di hosting che gestiscono i grandi aggregatori o dai motori di ricerca diano luogo ad un intervento sui contenuti memorizzati o linkabili, tale da far veramente eccedere la neutralità della condotta del prestatore.

Al fine di rendere meglio percepibile questa situazione di incertezza, cui la costruzione della figura del provider attivo rischia di dar luogo è anche la mancanza di uniformità di interpretazione giurisprudenziale al riguardo.

Paradigmatico è proprio l'esempio del servizio di autocompletamento offerto da Google, che ha dato luogo al già menzionato disaccordo interpretativo in ambito giurisprudenziale.

Nella situazione così descritta, nella quale non è obiettivamente possibile comprendere cosa significhi, da un punto di vista strettamente tecnico, fornire funzionalità che eccedano un intervento meramente neutro e passivo, è evidente che il rischio maggiore è quello di provocare un pericolosissimo *chilling effect* nei confronti dei gestori delle piattaforme digitali (aggregatori ugc, blog, social network) e dei motori di ricerca, intimoriti dal fatto che la prestazione di servizi ormai difficilmente rinunciabili per la miglior fruizione e reperimento dei contenuti sulla rete possa comportarne la responsabilità secondo le regole ordinarie (art. 2043 c.c. nel nostro ordinamento), stante la fuoriuscita dal *safe harbour* rappresentato dalle disposizioni di cui agli artt. 14-16 del d.lgs. n. 70 del 2003.

E' quindi auspicabile che il legislatore europeo si appresti con sollecitudine alla revisione ed adeguamento della direttiva 2000/31, peraltro già prevista dall'art. 21 della direttiva, al fine non solo di introdurre procedure armonizzate di *notice and take down* (come pare essere nei piani della Commissione, stando ad alcune posizioni espresse nel 2012 con riguardo all'attualità o meno della direttiva in argomento) ma di intervenire anche in tema di regole di responsabilità dei motori di ricerca e delle attuali, più evolute figure di *host provider*, che non rispondono più certamente a quelle conosciute all'epoca della redazione della direttiva (anni 1998-2000).

Si tratta, ad avviso di chi scrive, di un intervento non eludibile, nel cui ambito dovranno essere necessariamente chiariti anche i confini di quella più volte citata neutralità che rappresenta il fondamento della operatività del regime speciale di cui agli artt. 12-14 direttiva e 14-16 d.lgs. n. 70 del 2003.

Ad avviso di chi scrive, infatti, la neutralità del servizio dell'*host provider* permane sino a che non divenga possibile affermare – ancora una volta dal punto di vista tecnico – che il suo intervento (indicizzazione, categorizzazione, ottimizzazione, autocompletamento, etc.) è tale da consentirgli un controllo sui contenuti immessi dagli utenti, perché solo tale consapevolezza potrebbe, forse, rendere superabile il basilare principio dell'assenza di un obbligo generale di sorveglianza (art. 15 direttiva e art. 17 d.lgs. n. 70 del 2003), il quale si giustifica e resiste fin tanto che la conoscenza dei contenuti immagazzinati si considera tecnicamente impossibile/inesigibile, o comunque eccessivamente gravosa²⁷.

²⁷ È assolutamente pacifico che il principio in questione sia stato introdotto dal legislatore europeo proprio per evitare di esporre i provider a forme oggettive o aggravate di responsabilità rispetto a contenuti che tecnicamente non è in grado di controllare. Sul punto si veda, in dottrina, PINO, Assenza di un obbligo generale di sorveglianza a carico degli internet service provider sui contenuti immessi da terzi in rete, in *Danno resp.*, 2004, 834; RICCIO, La responsabilità degli internet providers nel d.lgs. n. 70/2003, cit., 2003, 1158; sia anche consentito il rinvio a BUGIOLACCHI, La responsabilità dell'host provider, cit., 192.

Pertanto, sino a che non verrà attuata quella *technical disclosure* cui si faceva cenno sopra, la neutralità del servizio del provider non sembra ecceduta dalla prestazione degli innovativi, fondamentali servizi descritti, in quanto una cosa è pervenire a dei “risultati” di ricerca che richiamano contenuti memorizzati mediante programmi automatici, altra è ritenere che attraverso tali programmi il provider sia in grado di controllare il contenuto dei materiali immessi sulle piattaforme (o motori) da lui gestiti, così da perdere la “irresponsabilità” derivante dall’intero sistema degli artt. 12-15 direttiva, il quale parrebbe basato, come ricordato anche dalle decisioni della Corte di Giustizia, su una attività meramente passiva del provider.

Tale ultima considerazione suggerisce una ulteriore riflessione.

A ben vedere, il considerando n. 42) della direttiva, richiamato sia dalla Corte europea che dai giudici italiani i quali all’interpretazione del giudice sovranazionale compiono riferimento, afferma che il regime speciale di responsabilità del prestatore di servizi della società dell’informazione riguarda esclusivamente il caso in cui l’attività di prestatore si limiti al processo tecnico di attivare e fornire accesso ad una rete di comunicazione sulla quale sono “trasmesse o temporaneamente memorizzate le informazioni messe a disposizione da terzi al solo scopo di rendere più efficiente la trasmissione. Siffatta attività è di ordine meramente tecnico, automatico e passivo, il che implica che il prestatore di servizi della società dell’informazione non conosce né controlla le informazioni trasmesse o memorizzate”.

Nel far ciò pare di poter dire che le tipologie di servizio alle quali si riferisce il considerando in parola sembrano essere esclusivamente quelle poi qualificate dagli artt. 12 e 13 della direttiva come, rispettivamente, di *mere conduit* e *caching*, e non anche a quelle di hosting: il riferimento all’accesso, alla trasmissione o alla memorizzazione temporanea (identificativa del *caching*) fanno allora pensare che l’operatività delle condizioni di responsabilità (o di esonero da essa, a seconda della prospettiva di analisi che si preferisca) dell’*host provider*, di cui all’art. 14 direttiva e 16 d.lgs.n. 70/2003 non sia indissolubilmente legata al carattere strettamente neutro della sua attività. Potrebbe quindi ipotizzarsi che il legislatore europeo, che già all’epoca della redazione della direttiva aveva presenti i possibili, futuri sviluppi della prestazione dei servizi resi dai provider (tanto da menzionare espressamente i motori di ricerca, pur non oggetto di disciplina, nell’articolo 21, dedicato alla revisione della direttiva), abbia implicitamente ritenuto che i servizi di hosting, ai quali, secondo l’opinione maggioritaria sono da ricondurre i motori di ricerca ma ai quali, senza dubbio alcuno si devono ricondurre i servizi di memorizzazione dei grandi aggregatori di contenuti, postulino, per il loro stesso efficiente funzionamento, interventi anche non meramente passivi, a condizione che essi non si traducano, come già accennato, in una concreta possibilità tecnica di controllo sui contenuti. Diversamente, non si comprenderebbe come mai il *considerando* 42) non abbia menzionato anche, ai fini delle condizioni di applicabilità delle deroghe alla responsabilità, il servizio di memorizzazione “puro” (permanente), e non meramente temporaneo, che connota inequivocabilmente l’attività di hosting.

Tale impostazione, per giunta, ci pare possa essere corroborata anche dal testo del considerando n. 43), il quale ugualmente, nello specificare i presupposti della limitazione di responsabilità si riferisce ancora espressamente, e altrettanto inequivocabilmente, alle sole attività di *mere conduit* e di *caching*²⁸.

²⁸ Secondo il considerando n. 43) “Un prestatore può beneficiare delle deroghe previste per il semplice trasporto (“*mere conduit*”) e per la memorizzazione temporanea detta “*caching*” se non è in alcun modo coinvolto nell’informazione

Infine, ancora l'art. 21 della direttiva, dedicato al c.d. “riesame” biennale della direttiva, al secondo comma, scinde nettamente la responsabilità dei fornitori di servizi di motori di ricerca ed host provider (non nominati espressamente, ma richiamati grazie all'inequivoco riferimento alle procedure di *notice and take down*, tipiche di quella attività), da quella dei prestatori di *mere conduit* e di *caching*.

Quanto appena detto, quindi, dovrebbe indurre ad una revisione della direttiva che contenga un aggiornamento e/o integrazione delle ipotesi di responsabilità dei provider, anche alla luce delle nuove funzionalità offerte.

Solo un ulteriore intervento armonizzatore di questo tipo potrebbe consentire di realizzare un corretto bilanciamento tra libertà di manifestazione del pensiero e circolazione della conoscenza da un lato e tutela dei diritti della persona e sulle opere protette dall'altro.

trasmessa...”.

OPEN DATA E DATA PROTECTION NEL CLOUD COMPUTING

Alberto Maria Gambino

 *Multimedia*



Clicca sull'immagine o fotografa il QrCode
per accedere al MediaBook CLIOedu

CLOUD COMPUTING E TRATTAMENTO DEI DATI SANITARI

Massimo Farina

 *Multimedia*



Clicca sull'immagine o fotografa il QrCode
per accedere al MediaBook CLIOedu

LA GIUSTIZIA TELEMATICA

Irene Sigismondi

 *Multimedia*



Clicca sull'immagine o fotografa il QrCode
per accedere al MediaBook CLIOedu

NET NEUTRALITY

LA NEUTRALITÀ DELLA RETE: PROBLEMI ATTUALI E PROSPETTIVE

Angela Viola

 *Multimedia*



Clicca sull'immagine o fotografa il QrCode
per accedere al MediaBook CLIOedu

Abstract: *We present the origins and evolution of the Internet, with special focus on the normative distinction between carriers/ network operators and content providers. We analyze a possible definition of net neutrality, since the technological neutrality principle in the EU universal access directive of 2002. We consider the “Connected Continent” EC regulation proposal, which aims at introducing a specific incentive for quality of services in the normative framework, in order to foster competition and protect consumers’ rights. We conclude with some critical perspectives on the issue, also considering some aspects of the US debate.*

Parole chiave: Neutralità della rete – rete aperta – Internet – regolazione di Internet – servizi a qualità garantita

Keywords: *Internet regulation – net neutrality – quality of service.*

Sommario: 1. Inquadramento ed evoluzione - 2. La scissione normativa contenuti/infrastrutture - 3. Evoluzione normativa sull’infrastruttura - 4. Cenno alla regolazione dei contenuti in rete - 5. La neutralità della rete: attualità - 6. La proposta di regolamento sulla *net neutrality* - 7. Problematiche giuridiche e tecniche: i servizi a qualità garantita possono limitare la neutralità della rete Internet? Un cenno alla tematica negli USA - 8. *Internet* come rete aperta e libera: prospettive critiche

1. Inquadramento ed evoluzione

Il senso di questa espressione è strettamente connesso al doppio significato della rete stessa, intesa come contenuto e come canale e nello specifico come mezzo, come medium, proprio per intendere la modalità con cui il messaggio viene trasmesso e circola sulla rete stessa.

Il significato è quello letterale: la rete come entità neutrale: in che senso?

Collegiamo questo concetto a quello di rete aperta: la caratteristica originaria di Internet si concretizza proprio nella possibilità di veicolare qualsiasi informazione che possa essere trasformata in una sequenza di bit (digitalizzazione), soprattutto ora che le potenzialità tecniche sono aumentate grazie alla tecnologia della banda larga¹.

A questa caratteristica, la neutralità, come principio, aggiunge che la circolazione sulla rete di queste sequenze di bit, deve avvenire, per quanto più possibile, in regime di parità di trattamento, ossia alle stesse condizioni.

Ora, questa potenzialità era stata individuata come tratto essenziale di Internet già nella storica sentenza della Corte Federale del Distretto della Pennsylvania sul Communications Decency Act del 1996, che espone le caratteristiche della rete Internet². La grandezza di Internet sta proprio nel fatto che si tratta di una rete aperta, che permette una interconnessione tale da consentire, come

¹ L’evoluzione tecnologica ha consentito di passare da una connessione analogica alla rete attraverso i cavi telefonici tradizionali, ad una connessione digitale via via sempre più “potente”, grazie alla velocità di trasmissione di pacchetti di dati di dimensioni sempre maggiori. Queste connessioni, che hanno diverse tipologie di specifiche tecniche, vengono definite sinteticamente “a Banda Larga”, ma la tecnologia, in continua evoluzione, impone anche una riflessione di carattere giuridico. Sono richiesti forti investimenti al riguardo, che, di fatto, soltanto soggetti già presenti in misura rilevante sul mercato della rete possono realizzare, e ciò con evidente compromissione dei principi della concorrenza, parità di accesso al mercato e, di conseguenza, di neutralità della rete rispetto ai servizi che vi transitano.

² Si veda: Dir. informaz. e informatica, 1996, 604 ss. con nota di V. ZENO ZENCOVICH.

presupposto filosofico, a chiunque l'accesso e la "manifestazione" del proprio pensiero, e, come risolto pratico, la trasmissione potenzialmente indifferente (neutrale) *sia* rispetto al mittente, *sia* rispetto al destinatario e *sia* rispetto al contenuto di dati e informazioni distribuite in pacchetti che viaggiano sulla rete a qualunque titolo (es. traffico dati, voce, "televisione").

Volendo enucleare il concetto di apertura della rete, va messo in evidenza come la rete si caratterizzi proprio per l'assenza di un "dominio incontrastato di un centro" a favore di una "pluralità di centri interconnessi tra loro", realizzando così una reciprocità di connessioni, dove chi è fornitore di una informazione può essere al contempo destinatario di informazioni trasmesse da altri³.

2. La scissione normativa contenuti/infra-strutture

La doppia valenza di Internet, per quanto si configuri come strettamente compenetrata dell'uno e dell'altro aspetto, il contenuto e il mezzo, si presenta, dal punto di vista della regolamentazione, scissa.

Infatti, la doppia valenza, di mezzo e contenuto, oltre ad influire sull'approccio alla comunicazione interpersonale⁴, ha imposto una diversificazione, dal punto di vista giuridico, dei soggetti che operano sulla rete a vario titolo.

Mentre l'operatore di rete (*network operator*) utilizzando il mezzo, segue la scia della disciplina tradizionale delle infrastrutture, che, almeno in linea di principio, si rinviene nella direttiva quadro sulle comunicazioni elettroniche e successivi interventi di aggiornamento, per quanto attiene al fornitore di servizi (*service provider* e, nello specifico ISP: *Internet Service Provider*) è stata più forte l'influenza del *medium* telematico e tale peculiarità si è riverberata proprio nella normativa della società dell'informazione, come è accaduto, per esempio, nella disciplina dell'e-commerce, sempre però a partire da principi generali condivisi tra i diversi ordinamenti dell'UE.

Infatti, dal punto di vista giuridico della tutela, il legislatore è intervenuto utilizzando le categorie tradizionali, solo però dopo averle adattate alle particolari modalità della comunicazione elettronica⁵.

³ In questa prospettiva e traslando il discorso a livello filosofico, sorge il problema se e come tutto ciò comporti il dissolvimento del concetto tradizionale di modello giuridico con "univoco" fondamento, e la sua trasformazione in sistema "multilivello" o "plurale".

⁴ Si pensi, dal punto di vista sociologico all'influsso dei *social networks* sulle modalità di comunicazione delle giovani generazioni, che prescindono quasi dal contatto fisico. L'approccio interpersonale cambia e, a cascata, coinvolge anche le generazioni non "native digitali" contribuendo a colmare il *digital divide*.

⁵ Anche in ragione dei concetti di proposta e accettazione, categorie generali appartenenti alla tradizione giuridica, è possibile evidenziare come il legislatore abbia voluto, anche nell'ambito di questo nuovo contesto di riferimento del commercio elettronico, utilizzare un *fictione juris* che ricollega l'effetto dell'accettazione alla mera possibilità di accesso alle relative comunicazioni, come disciplinato nell'art. 13 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. In tal modo, queste nuove modalità di acquisizione della volontà contrattuale, mediante l'utilizzo dei servizi della società dell'informazione disponibili sulla rete, divengono, a loro volta, categorie generali connesse al tipo di strumento utilizzato (ad es. il telefonino, la tv digitale, il traffico dati). Da qui, la necessità di diversificare le discipline giuridiche nei singoli Stati membri, ma con l'esigenza però anche un coordinamento unico dell'UE.

3. Evoluzione normativa sull'infrastruttura

Prima di formulare una definizione di “neutralità”, ci soffermiamo sul concetto di “apertura” della rete, che ne sta alla base come presupposto.

Anzitutto, la caratteristica di rete aperta, implica la sussistenza delle categorie distintive e peculiari rappresentate da a-territorialità e real-time, che possono configurare la virtualità come meta-categoria. La prima, (a-territorialità) consiste nella mancanza di un vincolo di tipo territoriale e, di conseguenza statutale: infatti uno dei principi cardine, costitutivi 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 (real time): ogni tipo di comunicazione avviene virtualmente in modo contestuale, in tempo reale.

Tale caratteristica di rete aperta, anche rispetto alle categorie spazio-temporali, impone anche una riflessione sulle peculiarità che ne seguono come corollario, dal punto di vista giuridico, ancora una volta, legate a questa doppia valenza di Internet, come mezzo e contenuto, a vari livelli.

Inizialmente, il legislatore comunitario ha introdotto (2000) una normativa *relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno*, come recita la direttiva 2000/31/CE, che disciplinava il c.d. commercio elettronico, dunque ha regolato la materia e quindi il contenuto.

Poi, nel 2002, è intervenuta una disciplina generale sull'infrastruttura, con la direttiva quadro sulle comunicazioni elettroniche (2002/21/CE), cui si aggiungono, nella previsione della convergenza tra diverse modalità di comunicazione, anche le ulteriori direttive specifiche del settore (autorizzazioni, accesso, servizio universale, privacy)⁶. Tuttavia, questa stessa normativa volutamente non ha disciplinato l'aspetto dei contenuti delle comunicazioni veicolate nella/dalla rete⁷.

Quanto al mezzo, e quindi alla rete, la versatilità, la polifunzionalità delle tecnologie, intesa come capacità di rapido sviluppo, ha consentito di fornire contestualmente svariati tipi di servizi,

⁶ Direttiva 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») a cui si aggiungono le Quattro direttive specifiche del settore: quattro direttive specifiche, ossia: la direttiva relativa all'autorizzazione per le reti e i servizi di comunicazione elettronica (direttiva “autorizzazioni”); la direttiva relativa all'accesso alle reti di comunicazione elettronica e delle risorse correlate e alla loro interconnessione (direttiva “accesso”); la direttiva relativa al servizio universale (direttiva “servizio universale”); la direttiva sul trattamento dei dati personali (direttiva “vita privata e comunicazioni elettroniche”).

⁷ Nella citata direttiva quadro, al considerando (5) si legge: “Di conseguenza, il presente quadro normativo non si applica ai *contenuti* (corsivo mio) dei servizi forniti mediante reti di comunicazione elettronica che utilizzano servizi di comunicazione elettronica, come i contenuti delle emissioni radiotelevisive, i servizi finanziari e taluni servizi della società dell'informazione e lascia quindi impregiudicate le misure adottate a livello comunitario o nazionale riguardo a tali servizi in ottemperanza alla normativa comunitaria, per promuovere la diversità culturale e linguistica e per assicurare la difesa del pluralismo dei mezzi di informazione. Il contenuto dei programmi televisivi è disciplinato dalla direttiva 89/552/CEE del Consiglio del 3 ottobre 1989, relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri concernenti l'esercizio delle attività televisive. *La separazione della disciplina dei mezzi di trasmissione dalla disciplina dei contenuti non incide sul riconoscimento dei collegamenti fra i due aspetti, in particolare al fine di garantire il pluralismo dei mezzi di informazione, la diversità culturale e la protezione dei consumatori* (corsivo mio).”

attraverso l'evoluzione della c.d. banda larga, che può veicolare *indifferentemente* traffico di dati, traffico telefonico di tipo VoIP (*Voice over IP - Internet Protocol*), e televisione digitale di tipo IPTV (*Internet Protocol TeleVision*) etc. Ciò ha posto, di conseguenza, il problema del *se* diversificare la disciplina giuridica in base al tipo di servizio in questione, così che la diversificazione dei servizi ha, per certi versi, imposto una diversa disciplina giuridica, pur sempre in un quadro comune⁸, e, per altri, ha favorito aspetti di convergenza, ancora una volta nella logica del quadro normativo comune.

In altri termini, originariamente, la direttiva quadro (2002/21/CE) copriva tutte le problematiche attinenti alla disciplina generale “quadro” delle comunicazioni elettroniche come infrastruttura, salvo, come appena ricordato, rinviare ad altra normativa per la disciplina dei contenuti (considerando 5 della direttiva stessa).

Trattandosi di una direttiva, essa ha posto principi generali di armonizzazione per gli Stati membri, tra cui, per la prima volta, quello di “neutralità tecnologica”, di cui si parla espressamente al considerando 18 ed all'art. 8. Specificando, la direttiva ha imposto agli Stati membri l'obbligo di tenere “nel massimo conto l'opportunità di una *regolamentazione tecnologicamente neutrale* (corsivo mio), ossia che non imponga l'uso di un particolare tipo di tecnologia, né che operi discriminazioni tra particolari tecnologie”⁹. Del resto, la tecnologia stessa, nei confronti del diritto è sempre da considerare neutrale: essa può presentarsi al tempo stesso come “*trasparente*” o come “*scatola nera*”. La tecnologia è “trasparente” nei confronti dell'utente, nel senso che opera come interfaccia indifferente rispetto al risultato finale (ad es. il tipo di mezzo di trasporto è indifferente rispetto alla meta da raggiungere), ed è “scatola nera”, in quanto si presenta come strumento necessario a cui attingere solo nell'eventualità di cattivo funzionamento (ad es. in caso di incidente durante il trasporto diviene rilevante conoscere i dati registrati da vari sensori al fine di individuare come e dove si è verificato tecnicamente un eventuale guasto).

Si tratta dunque di una prima definizione normativa di neutralità tecnologica (da cui poi deriva anche quella di neutralità della rete) come principio generale, non assoluto (“*tenere nel massimo conto*”) di cui si prevede già in partenza la possibilità di deroga nelle stesse discipline nazionali di dettaglio dei singoli servizi. Così, l'obbligo di tenere nel massimo conto la neutralità tecnologica “non preclude l'adozione di provvedimenti ragionevoli volti a promuovere taluni servizi specifici, ove opportuno, per esempio la televisione digitale come mezzo per aumentare l'efficienza dello spettro”. Ciò si è effettivamente realizzato in ambito comunitario¹⁰.

⁸ Tale distinzione si inserisce comunque nel “quadro comune” di riferimento, ossia la direttiva 2002/21/CE, consentendo così, in assenza di specifiche regolamentazioni, di poter fare ricorso ai canoni interpretativi classici dell'interpretazione estensiva, trattandosi, pur con le dovute precisazioni, della stessa materia (*eadem ratio*).

⁹ Il considerando 18 pone sia il principio generale (neutralità tecnologica) sia la deroga: “L'obbligo per gli Stati membri di garantire che le autorità nazionali di regolamentazione *tengano nel massimo conto l'opportunità di una regolamentazione tecnologicamente neutrale* (corsivo mio), ossia che non imponga l'uso di un particolare tipo di tecnologia né che operi discriminazioni tra particolari tecnologie, non preclude l'adozione di provvedimenti ragionevoli volti a promuovere taluni servizi specifici, ove opportuno, per esempio la televisione digitale come mezzo per aumentare l'efficienza dello spettro.” Lo stesso principio viene ribadito nell'art. 8 del testo della Direttiva.

¹⁰ Lo spettro radio è la gamma di radio-frequenze che possono essere allocate in modo diverso per diversi servizi (per esempio telefonia cellulare, dispositivi di controllo a distanza come l'apertura delle porte automatizzata, la sorveglianza dei neonati, fino ai sistemi di posizionamento globale). Il concetto di spettro-radio è strettamente connesso alla modalità con cui vengono distribuite le radio-frequenze, trattandosi oggi di una delle infrastrutture

Tuttavia, la stessa struttura (principio generale con deroga) che inizialmente ha interessato la disciplina dei servizi da parte degli Stati membri, ha poi caratterizzato anche l'approccio comunitario. Infatti, all'interno del "quadro" normativo generale sono state apportate delle deroghe ulteriori nello stesso ambito comunitario per settori specifici, di cui si è anche prevista la revisione periodica (art. 25 dir. 2002/21/CE).

Proprio da questa linea di sviluppo, è scaturito, successivamente, il nuovo quadro normativo del 2009, in risposta all'ulteriore evoluzione tecnologica dell'infrastruttura, ossia la rete, ed alla crescente eterogeneità dei servizi offerti in rete. Di conseguenza, sempre in risposta alle esigenze del mercato unico/interno, la scelta normativa dell'Unione Europea è diretta alla tutela della concorrenza ed alla tutela dei consumatori e sceglie lo strumento della direttiva, che garantisce il rispetto delle competenze di settore dei singoli Stati membri, assicurando al contempo l'uniformità della disciplina generale.

In questo senso, si pensi al caso della telefonia.

Il legislatore comunitario, stante l'eterogeneità delle tipologie di servizi e delle relative tariffe tra i diversi Stati membri, ha dovuto introdurre un regolamento specifico in materia di *roaming* telefonico intracomunitario, (*Regolamento (CE) n. 717/2007 relativo al roaming sulle reti pubbliche di telefonia mobile all'interno della Comunità e che modifica la direttiva 2002/21/CE*) che ha operato dei correttivi alla disciplina dei sistemi tariffari "voce" (c.d. euro-tariffa) tra i diversi paesi.

Si introduce così una deroga alla direttiva-quadro che produce effetti per un periodo di tempo limitato¹¹, attraverso la scelta della fonte normativa regolamentare: tale scelta risponde all'esigenza di applicazione diretta e di immediata efficacia nei confronti di tutti gli Stati membri, senza necessità di normative di adeguamento, come avviene per il caso della direttiva. Inoltre, il regolamento rappresenta lo strumento più idoneo in base al principio di sussidiarietà, in quanto garantisce una disciplina uniforme della materia senza coinvolgere il potere decisionale degli Stati membri, che pure conservano la rispettiva competenza in materia. Infatti, in tal modo, l'intervento dell'Unione Europea si palesa come una modalità di coordinamento per la salvaguardia del mercato e dei consumatori nel settore. Ciò corrisponde anche all'esigenza di attuare il principio di proporzionalità che si manifesta, invece, nello specifico, mediante l'idoneità del mezzo regolamentare, superando, in via preventiva, gli eventuali ostacoli di politica legislativa, e le pericolose differenziazioni nell'ambito della disciplina di dettaglio, che una direttiva avrebbe potuto (pericolosamente) incontrare, in termini di necessaria armonizzazione successiva, da parte degli Stati membri¹².

chiave per le telecomunicazioni in genere e quindi anche per le comunicazioni elettroniche. Le radio-frequenze possono essere assegnate a ciascun servizio in modo significativamente diverso da un paese all'altro, in quanto la competenza appartiene ad ogni singolo Stato membro. Tutto ciò determina il fatto che, a livello normativo vi siano differenze tra gli Stati a seconda di esigenze nazionali ed importanza attribuita ai differenti servizi che usano le radioemissioni. È sorta da subito, quindi, la necessità di coordinamento da parte dell'UE. Infatti, al di là dell'aspetto tecnologico, poiché si tratta di risorse scarse, nel decidere gli usi e gli utilizzatori dello spettro radio è necessario arrivare a bilanciamenti e dunque rileva l'approccio giuridico a livello comunitario e l'esigenza di affrontare normativamente anche il problema tecnologico. Ad esempio, uno specifico caso è quello della transizione nell'Unione Europea dalla tv analogica a quella digitale. Per il passaggio (*switchover*) dall'analogico al digitale e la chiusura (*switch-off*) della tv analogica, infatti, ci sono stati diversi interventi di coordinamento a livello comunitario, normativi e strategici: COM(2003)(541), (COM(2005)204) (strategie del *switchover*) COM(2009) 586 and C(2009) 8287.

¹¹ Cfr. considerando 39, id.

¹² Cfr. considerando 38 reg. 2007/717.

Ecco dunque che la regolamentazione giuridica stessa viene a diversificarsi in base alla tipologia di servizio offerto in rete, sicuramente in modo unitario e standardizzato, grazie, come si diceva, alla scelta dello strumento del regolamento comunitario, ma anche in deroga alla disciplina generale posta dalla direttiva-quadro, proprio come in un rapporto tra *species* e *genus*. Questa modalità prescelta (regolamento *vs* direttiva) risponde al fatto che l'obiettivo è il raggiungimento di un mercato interno/unico nel settore delle comunicazioni ed è anche garanzia di tutela della concorrenza e dei consumatori, e che, in altri termini, rappresenta una specifica articolazione dell'obiettivo primario dell'Unione Europea.

L'eterogeneità dei servizi, dunque, ha imposto, da subito, una diversa regolamentazione e disciplina giuridica. Tale deroga, sempre con gli stessi presupposti e finalità, è stata poi ampliata anche nell'ambito della fornitura in roaming di servizi SMS e dati all'interno della Comunità (Regolamento (CE) N. 544/2009 e Regolamento (UE) n. 531/2012).

Riassumendo, la *ratio* comune ad entrambi questi provvedimenti normativi, è quella di creare misure temporanee, volte al riequilibrio del mercato interno/unico per la tutela della concorrenza e degli utenti, e l'*eadem ratio* sta, come vedremo, anche alla base della proposta di regolamento sulla *net neutrality*.

4. Cenno alla regolazione dei contenuti in rete

Quanto al contenuto che può circolare sulla rete, si impone la riflessione su ciò che giuridicamente sia lecito e ciò che non lo sia in questa specifica modalità di comunicazione elettronica¹³.

In questa ottica, il legislatore comunitario, sin dalla direttiva 2000/31/CE, si è occupato della gestione della responsabilità nelle tre figure di fornitore di servizi della società dell'informazione, introducendo diversi livelli di responsabilità con i relativi profili. All'attività di mero trasporto, di *caching* e di *hosting* corrispondono tre forme di responsabilità del *provider*¹⁴.

Senza entrare nello specifico, in sintesi, viene messo in rilievo il potere di controllo o di supervisione come elemento discriminante per individuare una qualche forma di responsabilità. Peraltro, se questo era lo scenario di partenza introdotto dal legislatore comunitario, è necessario registrare un'attuale tendenza a dare ancor maggiore rilievo alla effettiva capacità dell'*Internet Server Provider* di prendere conoscenza *attiva* del contenuto dell'informazione che transita sulla rete per suo tramite¹⁵.

¹³ Tra le prime comunicazioni relativi alla disciplina del fenomeno Internet, troviamo una Comunicazione al Parlamento europeo, al Consiglio, al Comitato economico e sociale ed al Comitato delle regioni, datata 16/10/96 COM(96) 487, dal titolo "*Informazioni di contenuto illegale e nocivo su Internet*", da cui emerge, in buona sostanza, il principio guida che ciò che è lecito fuori dalla rete è lecito in rete.

¹⁴ Cfr., per l'attuazione della direttiva comunitaria 2000/31/CE nel nostro ordinamento gli artt. 14, 15 e 16 del D. Lgs. 70/2003.

¹⁵ Cfr. fra gli altri, per l'ipotesi di uso del marchio come parola chiave per le ricerche in rete, le decisioni della Corte di Giustizia nei casi Google France & Google Inc. e altri contro Louis Vuitton Malletier (C-236-7-8/08, sent. 23/03/2010), L'Oréal S.A. e altri contro eBay International AG e altri (C-234/2009, sent. 12/07/2011).

5. La neutralità della rete: attualità

Dunque tornando al concetto di neutralità della rete, alla luce anche di queste riflessioni di partenza, si può tentare una prima definizione attuale, da cui emerge come il primo elemento di questo concetto sia strettamente connesso all'essenza stessa della rete, concepita come *rete aperta*, caratteristica giuridicamente irrinunciabile, per cui ogni tentativo di "contenerla" significherebbe snaturare tale caratteristica.

Il secondo elemento per definire il concetto di neutralità deriva in effetti dal primo: attraverso la rete *qualsiasi contenuto* può essere veicolato e non è possibile "aprioristicamente" filtrarlo in alcun modo. Questo principio è, prima ancora che giuridico, di matrice squisitamente tecnica, dal momento che l'infrastruttura di rete (il mezzo) consente, in astratto, il passaggio di qualsiasi tipologia di informazione (il contenuto) rendendola neutrale nei confronti dei destinatari. A corollario di quanto evidenziato, è possibile riconoscere nel disposto dell'art. 15 della direttiva 2000/31/CE, rubricato "*Assenza dell'obbligo generale di sorveglianza*", un *quasi*-divieto di controllo generale¹⁶, in relazione ai "contenuti" che transitano sulla rete. Anzitutto non sussiste, e, da un punto di vista di etica legislativa, forse neppure potrebbe sussistere, un obbligo generale di sorveglianza o, peggio ancora, un "*obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite*", viceversa necessita un obbligo di cooperazione dei prestatori di servizi della società dell'informazione che sono "*tenuti ad informare senza indugio la pubblica autorità competente di presunte attività o informazioni illecite dei destinatari dei loro servizi o a comunicare alle autorità competenti, a loro richiesta, informazioni che consentano l'identificazione dei destinatari dei loro servizi con cui hanno accordi di memorizzazione dei dati*" (cfr. art. 15 Dir. 2000/31/CE cit.). Ma v'è di più: dal combinato disposto delle direttive 2004/48/CE e 2002/58/CE emerge che il diritto comunitario "non osta a che gli Stati membri istituiscano un obbligo di comunicazione a soggetti privati terzi di dati personali relativi al traffico al fine di consentire l'avvio di procedimenti civili per violazioni del diritto d'autore"¹⁷. Si tratta dunque di una scelta discrezionale in capo alle legislazioni di recepimento da parte degli Stati membri.

Anche la giurisprudenza comunitaria ha evidenziato questo principio, con riferimento specifico al problema del c.d. filtraggio dei contenuti. Al riguardo, ha individuato alcune problematiche cruciali: in primo luogo che la predisposizione di un sistema di filtraggio renderebbe obbligatorio il rispetto della normativa sul trattamento dei dati personali e sul segreto delle comunicazioni. In secondo luogo, che tale sistema risulterebbe comunque non conforme all'esigenza di garantire il giusto equilibrio tra protezione di posizioni giuridiche soggettive tutelate e libertà d'impresa. Nello specifico, il contrasto si registrava tra il diritto di proprietà intellettuale, di cui godono i titolari dei diritti d'autore, nei confronti della libertà di impresa di cui beneficiano gli operatori come i

¹⁶ In un'ottica di teoria generale del diritto, l'*assenza di un obbligo generale* si può ricondurre alle tematiche dei modi deontici fondamentali, che si riducono alle tre modalità *obbligatorio, vietato e facoltativo o permesso*. Si veda in tal senso F. Modugno, *Lineamenti di teoria del diritto oggettivo*, Milano, 2009, pp. 13 ss. Nella valutazione della fattispecie, sembrerebbe quasi, utilizzando un canone tipico della teoria generale del diritto, che il legislatore comunitario abbia scelto volontariamente di non porre un divieto giuridico assoluto, in senso forte, proprio al fine di favorire la cooperazione con le pubbliche autorità da parte dei prestatori di servizi.

¹⁷ Cfr. la decisione sul caso C-557/07 – *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten* della Corte di Giustizia dell'Unione Europea del 19/02/2009.

prestatori di servizi di *hosting*¹⁸.

Appare quindi evidente la stretta connessione/collegamento tra il concetto giuridico di neutralità e quello tecnologico, in cui la direzione è univoca, perché la neutralità è quella tecnologica, mentre quella giuridica è una tensione, una “*factio*” come obiettivo fissato dal legislatore, che quindi è derogabile. Alla molteplicità di strumenti tecnologici che possono in effetti consentire la fruizione di informazioni e servizi sulla rete possono corrispondere più discipline o anche una sola, a seconda delle scelte del legislatore.

Ciò si è verificato nell’evoluzione normativa con riferimento alla riforma del quadro normativo sulle comunicazioni elettroniche del 2009¹⁹, in cui il legislatore comunitario, dopo aver nuovamente proclamato i principi guida del mercato²⁰, si sofferma su un settore specifico delle comunicazioni elettroniche: quello legato alle radio-frequenze, che, come si esprime il cons. 24 “dovrebbero essere considerate una risorsa pubblica molto limitata, che ha un importante valore pubblico e di mercato”.

A ben guardare, dunque, questa direttiva consente una doppia valenza giuridica della normativa. Rispetto alla tutela del mezzo, la normativa si pone come *programmatica*. Infatti, in calce alla Direttiva è presente una *Dichiarazione della Commissione sulla neutralità della rete*²¹.

¹⁸ Si vedano, oltre al caso sopra citato, ad esempio, i due casi che coinvolsero la Società Belga Autori-Editori: *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) contro Netlog NV* (CGUE sent. 16/02/2012, caso C-360/10) e *Scarlet Extended SA contro Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* (CGUE sent. 24/11/2011, caso C-70/10). Il dibattito su questa tematica è acceso, cfr. da ultimo la causa *Causa C-314/12, (UPC Telekabel Wien GmbH contro Constantin Film Verleih GmbH e Wega Filmproduktionsgesellschaft GmbH)* e le conclusioni dell’avvocato generale Pedro Cruz Villalón che ritiene di rispondere in senso affermativo, affidando il contemperamento dei diritti ai singoli Stati membri, al quesito centrale “se sia compatibile con il diritto dell’Unione, in particolare con la necessità di operare un bilanciamento dei diritti fondamentali delle parti coinvolte, vietare a un fornitore di accesso a Internet in modo totalmente generale (dunque senza la prescrizione di misure concrete) di consentire ai suoi clienti l’accesso a un determinato sito Internet fintanto che ivi siano, esclusivamente o prevalentemente, resi accessibili contenuti senza l’autorizzazione dei titolari dei diritti, qualora il fornitore di accesso a Internet possa evitare sanzioni per la violazione di tale divieto dimostrando di avere comunque adottato tutte le misure ragionevoli”.

¹⁹ Direttiva 2009/136/CE: “modifica della direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica, della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e del Regolamento (CE) n. 2006/2004 sulla cooperazione tra le Autorità nazionali responsabili dell’esecuzione della normativa a tutela dei consumatori”; e direttiva 2009/140/CE: “modifica alle direttive 2002/21/CE che istituisce un quadro normativo comune per le reti ed i servizi di comunicazione elettronica, 2002/19/CE relativa all’accesso alle reti di comunicazione elettronica e alle risorse correlate, e all’interconnessione delle medesime e 2002/20/CE relativa alle autorizzazioni per le reti e i servizi di comunicazione elettronica”.

²⁰ Cfr. considerando 23, Dir. 2009/140.

²¹ Eccone il testo: *Dichiarazione della Commissione sulla Neutralità della Rete*:

La Commissione ritiene che sia della massima importanza conservare l’apertura e la neutralità di Internet, tenendo pienamente conto della volontà dei legislatori di:

- *dichiarare la neutralità della rete come obiettivo politico e principio della regolamentazione* che dovrà essere promosso dalle autorità nazionali di regolamentazione,
- *rafforzare i correlati requisiti di trasparenza e*
- *conferire strumenti di salvaguardia alle autorità nazionali di regolamentazione per prevenire il degrado dei servizi e intralci o rallentamenti del traffico sulle reti pubbliche*. La Commissione sorveglierà da vicino l’attuazione di queste disposizioni negli Stati membri, riservando una particolare attenzione al modo in cui sono tutelate le libertà dei cittadini europei sulla rete nella propria relazione sullo stato di attuazione al Parlamento europeo e al Consiglio. Nel frattempo, la Commissione sorveglierà l’impatto degli sviluppi tecnologici e del mercato sulle libertà della rete e riferirà al Parlamento europeo e al Consiglio, entro la fine del 2010, sulla necessità di adottare orientamenti supplementari;

In essa si evince che l'apertura e la neutralità di Internet sono obiettivi da perseguire attraverso la volontà dei co-legislatori, sia a livello comunitario che a livello di Stati membri. In questo senso, la neutralità della rete si pone come obiettivo politico e come principio di regolamentazione da promuovere attraverso le autorità nazionali di regolamentazione.

Rispetto alla tutela del contenuto, la norma è *direttamente precettiva*, perché propone il modello di neutralità con riferimento tecnico specifico al tema delle radio-frequenze e lo presidia attraverso le garanzie della concorrenza nel mercato. Infatti, “sebbene la gestione dello spettro resti di competenza degli Stati membri, solo la pianificazione strategica, il coordinamento e, se del caso, l'armonizzazione a livello comunitario possono garantire che gli utilizzatori dello spettro beneficino appieno del mercato interno e che gli interessi dell'Unione europea possano essere efficacemente difesi a livello globale” (cons. 28).

Da questa premessa, per la efficace modifica del sistema attuale di gestione e distribuzione dello spettro, la direttiva si muove per precisare il concetto di neutralità tecnologica anzitutto, in via precettiva, come opportunità per i fornitori del servizio²² ed in secondo luogo, in via programmatica, come principio fondamentale, così come si evidenzia nella citata Dichiarazione della Commissione sulla neutralità della rete, in calce alla direttiva stessa.

In relazione a questo, ed all'importanza dell'accesso a Internet come risorsa aperta e neutrale, si può qui anche accennare alla risoluzione ONU del 6 Luglio 2012 sulla promozione, protezione e godimento dei diritti umani su Internet, anche a tutela della libertà di pensiero, in cui il Consiglio per i Diritti Umani (*Human Rights Council*) fa espressamente riferimento al fatto che “l'esercizio dei diritti umani, in particolare del diritto alla libertà di espressione, su Internet sia un'istanza di interesse ed importanza crescente, atteso il rapido passo dello sviluppo tecnologico che consente agli individui di tutto il mondo di utilizzare le tecnologie dell'informazione e comunicazione - ICTs” derivandone 5 punti²³:

1. *Afferma* che ciò che è tutelato fuori dalla rete è tutelato anche nella rete, in particolare il diritto di libertà di opinione ed espressione, applicabile a prescindere dalle frontiere e con qualsiasi mezzo di scelta, conformemente alla disciplina dell'art. 19 della Dich. Univ. dei diritti umani.
2. *Riconosce* la natura globale e aperta di Internet come una forza che guida e accelera il processo di sviluppo nelle sue varie forme.
3. *Richiama* gli Stati alla necessità di promuovere e favorire l'accesso ad Internet e la cooperazione internazionale volta allo sviluppo di mezzi e strutture ICT in tutti i paesi.
4. *Incoraggia* particolari procedure perché queste tematiche siano attuate già al presente.
5. *Decide* di continuare ad enfatizzare la promozione, protezione e godimento dei diritti umani, inclusa la libertà di espressione, su Internet e con altre tecnologie, anche in ordine al come Internet sia un importante mezzo per sviluppare ed esercitare i diritti umani, in accordo con il suo programma di lavoro.

farà inoltre ricorso alle proprie competenze nell'ambito della vigente normativa in materia di concorrenza per far fronte alle pratiche anticoncorrenziali che possano insorgere.

²² Cfr. considerando 35, 40, 68, ripresi negli art. 7 *ter* 'Disposizioni di attuazione', nell'allegata Dichiarazione.

²³ Traduzione dal testo inglese ad opera dell'autore.

6. La proposta di regolamento sulla *net neutrality*

A questo riguardo, prenderemo in considerazione la proposta di regolamento del Parlamento Europeo e del Consiglio recante misure per il completamento del mercato unico europeo per le comunicazioni elettroniche e per realizzare un Continente Connesso (*Connected Continent*)²⁴.

La premessa di questa proposta è che, di fatto, il continente europeo risulta già, in massima parte, tecnologicamente connesso, pur con le dovute differenziazioni tra i singoli Stati membri, ma non ancora dal punto di vista giuridico²⁵.

Il panorama normativo presenta infatti una forte frammentazione tra i diversi Stati membri, che sembra addirittura accentuare quel fenomeno di “scissione” già individuato a proposito del rapporto tra mezzo e contenuto connaturato alla caratteristica della doppia valenza della rete Internet. Questa scissione determina anzitutto forti difficoltà per l’attuazione del mercato unico, in quanto implica come conseguenza livelli non uniformi di protezione e regolazione diversa. Dal punto di vista economico, per gli operatori di comunicazioni elettroniche, ciò si traduce in elevati costi di gestione e, per gli utenti finali (*end-users*), in mancati benefici con riferimento ai servizi potenzialmente fruibili in rete.

Tutto ciò ha portato alla recente proposta della Commissione Europea, che contiene, ancora una volta, un esplicito riferimento al rispetto del principio della neutralità tecnologica (*principle of technological neutrality*): ossia non si impone, né si discrimina rispetto all’uso di una particolare tecnologia a preferenza di altre (*type of technology*)²⁶. Tale definizione riecheggia quella già presente nella direttiva quadro sulle comunicazioni elettroniche (2002/21/CE), ma il dibattito concettuale e politico a livello europeo (e internazionale) si è notevolmente ampliato.

La Commissione europea aveva infatti pubblicato la comunicazione Apertura e neutralità della rete internet in Europa (*The open Internet and net neutrality in Europe*) del 19 aprile 2011, con cui sono stati ribaditi i principi di riferimento: concorrenza, quadro normativo delle telecomunicazioni in generale e le principali problematiche che impediscono ad oggi di realizzare un vero mercato interno/unico in questo settore²⁷, concludendo con l’impegno a preservare l’apertura di Internet, e a garantire il mantenimento di una rete robusta e accessibile a tutti.

Nelle conclusioni, inoltre, si evidenziava che “*la neutralità della rete riguarda una serie di diritti e principi sanciti dalla Carta dei diritti fondamentali dell’Unione europea, in particolare il rispetto della vita privata e familiare, la protezione dei dati personali e la libertà di espressione e di informazione. Per questo motivo qualsiasi proposta legislativa nel settore sarà soggetta ad una valutazione approfondita dell’impatto sui diritti fondamentali e della conformità alla Carta dei diritti fondamentali dell’Unione europea*”²⁸.

²⁴ 2013/0309 (COD).

²⁵ Il senso di questa espressione rimanda alla forte presenza di reti informatiche e telematiche all’interno dei singoli Stati dell’Unione Europea, che consentono ed agevolano l’interconnessione delle comunicazioni e dei traffici commerciali, anche, e sempre più, inter-nazionali / trans-nazionali. Da qui la necessità che la disciplina giuridica sia coordinata, consentendo la coesione normativa, anche come tensione verso una unità Europea nella dimensione politica.

²⁶ Cfr. punto 8 della proposta di regolamento cit.

²⁷ Le problematiche censite nel documento sono per es. il blocco di servizi in rete, la gestione del traffico secondo criteri stabiliti, la discrepanza tra velocità pubblicizzata e velocità reale.

²⁸ Cfr. Comunicazione “Apertura e neutralità della rete Internet in Europa” della Commissione, p. 10.

La questione è emersa, poi, anche a seguito di una serie di consultazioni che si sono susseguite in ambito comunitario sul tema di come realizzare un mercato unico delle comunicazioni elettroniche: si tratta di una *species* dell'ampio *genus*, tipicamente comunitario del passaggio da un mercato *comune* ad un mercato *unico*²⁹.

Le premesse di questa proposta di regolamento trovano una giustificazione forte proprio nell'urgenza di concretizzare il mercato unico europeo delle comunicazioni elettroniche, per lo sviluppo della concorrenza e la tutela del consumatore nel suo diritto di scelta, evitando una discrasia da cui le imprese possono trarre indebiti vantaggi³⁰ e, del pari, nell'esigenza di chiare regole sulla neutralità della rete.

Entrando nel merito, il documento di proposta contiene alcuni criteri di riferimento, una sorta di "fabbisogno normativo" per la realizzazione e lo sviluppo del c.d. Continente Connesso. Tali criteri possono essere sintetizzati in:

- semplificazione della regolazione per le società;
- maggiore coordinamento nell'uso dello spettro-radio, favorendo le tecnologie e gli investimenti per la banda larga, le reti di nuova generazione (NGN *New Generation Networks* come ad es. il 4G) e la nascita a livello europeo di società in rete integrate tra loro;
- standardizzazione dei profili di accesso ai servizi di rete a livello europeo per favorire la concorrenza;
- protezione dell'apertura di Internet, garantendo la neutralità, l'innovazione ed i diritti dei consumatori;
- progressiva eliminazione delle tariffe differenziate in materia di *roaming* al fine di eliminarle nel 2016, mediante politiche di incentivi e disincentivi;
- protezione del consumatore con linguaggio chiaro nei contratti, informazioni comparabili e maggiori diritti per cambiare il tipo di contratto o il fornitore di servizio (*provider*).

Il panorama normativo di riferimento rimane, in linea di principio, invariato: non ci sono novità in termini di regolazione, salvo il regime di autorizzazione unica UE (capo II, articoli da 3 a 7), per cui gli operatori che intendono fornire servizi in diversi Stati membri non devono più essere autorizzati in ciascuno Stato membro. Non vi sono cambiamenti nelle tariffe o nella configurazione dei provider di servizi di comunicazione elettronica, né si crea un'unica disciplina sulle licenze in materia di spettro-radio, che resta di competenza degli Stati membri, pur sotto il coordinamento dell'Unione Europea³¹.

Al tempo stesso, non è previsto un limite alla differenziazione dei servizi su Internet e proprio

²⁹ Mentre nell'ambito del mercato comune, lo Stato membro può ancora intervenire con autonoma disciplina, sempre nel coordinamento della materia predisposto dalla direttiva di armonizzazione (in questo caso la direttiva quadro e tutte le direttive del settore), l'obiettivo del mercato unico è invece quello di rendere omogenea la disciplina giuridica e consentire l'accesso ai mercati nazionali a parità di condizioni, garantendo in questo modo la progressiva realizzazione delle libertà fondamentali di circolazione di beni, servizi, persone e capitali in tutti i settori, come obiettivo principale dell'Unione Europea.

³⁰ Il documento fa riferimento al c.d. *regulatory arbitrage*, la pratica grazie alla quale le imprese possono sfruttare a proprio vantaggio le lacune normative (*loopholes*) nel sistema regolatorio al fine di scegliere una disciplina, che consente di eludere quella sfavorevole o non conveniente, una forma non consona di applicazione dei criteri di collegamento del diritto internazionale privato.

³¹ Cfr. la citata proposta di regolamento, Capo III "Input europei" – Sezione I: Coordinamento dell'uso dello spettro radio all'interno del mercato unico, negli artt. 8 e ss.

su quest'ultimo punto, si evidenzia la necessità di verificare la sussistenza ancora del concetto di neutralità in rete. Ci si chiede se la previsione, ormai in via di completamento, di una differenziazione dei servizi in rete, possa inficiare il concetto stesso di neutralità della rete. Questo perché diversificare i servizi implica che alla pluralità dell'offerta possa non corrispondere più quella neutralità dal punto di vista tecnologico, che era stata posta come principio generale e da "tenere nel massimo conto", sin dalla Direttiva 2009/140/CE.

La discussione, a questo punto, si sposta sul significato di differenziazione dei servizi in rete, per capire quanto questo possa ancora consentire la qualificazione di "parità di trattamento" per tutto ciò che circola sull'infrastruttura della rete.

Si torna dunque ancora al problema originario di Internet, che viene a presentarsi nelle sue diverse e nuove articolazioni: da un lato, l'esigenza di mantenere neutrale, aperta e libera la rete e dall'altro la possibilità di offrire servizi differenziati "a qualità garantita", come già si prevedeva con l'art. 22 della direttiva 2002/22/CE in materia di servizio universale, a cui corrisponde per il nostro Paese, l'art. 61 del Codice delle Comunicazioni Elettroniche (Decreto Legislativo 259/03).

In senso più tecnico, la definizione di "qualità del servizio" è fornita dall'Unione Internazionale delle Telecomunicazioni (ITU) come l'insieme dei requisiti di un servizio di telecomunicazioni, che corrispondono a determinate caratteristiche, esplicite o implicite, afferanti all'utente del servizio. La qualità del servizio viene quindi misurata in base ad una serie di parametri dimensionati sull'utente finale del servizio. Nella citata proposta di regolamento, la qualità del servizio entra in gioco con riferimento al "*prodotto connettività*", individuando quindi un livello intermedio tra l'infrastruttura e il contenuto. In particolare, l'articolo 19, della citata proposta, è rubricato "*Prodotto di connettività con qualità del servizio garantita*" ed indica, al par. 4, una serie di caratteristiche a cui il servizio deve corrispondere per essere considerato come "fornitura di un prodotto *europeo* di connettività con qualità del servizio garantita", in relazione all'accesso ad Internet ed ai servizi di comunicazione elettronica.

In questa ottica, il legislatore comunitario ha evidenziato tutta una serie di diritti a garanzia degli utenti finali³², per cui questi ultimi possono accedere ad Internet attraverso qualsiasi provider (fornitori di comunicazioni elettroniche al pubblico), anche stabiliti in un altro Stato membro, senza che siano applicati requisiti o condizioni di accesso o di uso discriminatori o tariffe maggiori, tranne che eventuali differenze siano oggettivamente giustificate (art. 21). Di seguito, se da una parte il legislatore comunitario riconosce la libertà di fornire e di usufruire di un accesso a Internet aperto, con una gestione ragionevole del traffico (art. 23), dall'altra viene riconosciuta la garanzia della qualità del servizio (art. 24), attraverso la trasparenza e pubblicazione delle informazioni e connessi obblighi contrattuali (art. 25-29), del tutto in linea con il quadro normativo della direttiva comunitaria 2000/31/CE sul commercio elettronico. Anche qui, i fornitori di comunicazioni elettroniche al pubblico sono tenuti alla pubblicazione, tranne che per le offerte negoziate individualmente, di informazioni trasparenti, comparabili, adeguate e aggiornate in merito ad una serie di aspetti, che specificano i capisaldi delle informative precontrattuali e contrattuali obbligatorie³³.

³² Si v. il Capo IV della proposta di regolamento in cui si enumerano i Diritti *armonizzati* degli utenti finali.

³³ La proposta di regolamento ripete che le informazioni devono essere fornite in "forma chiara, esaustiva e facilmente accessibile nella/e lingua/e ufficiale/i dello Stato membro in cui è offerto il servizio e sono aggiornate regolarmente" (art. 25 cit.)

A questo quadro si aggiungono le previsioni in materia di cambiamento di fornitore³⁴, che fissano principi armonizzati per le procedure di cambio di fornitore quali l'orientamento ai costi, la gestione del processo di passaggio a cura del fornitore ricevente e la risoluzione automatica del contratto con il fornitore cedente, nonché una serie di disposizioni organizzative e finali volte al coordinamento, anche in materia di poteri sanzionatori, tra Autorità Nazionali e Commissione Europea.

Tornando allo specifico tema oggetto di indagine, da un punto di vista operativo, a questi diritti "armonizzati" corrisponde, sul versante dei fornitori di comunicazioni elettroniche, la possibilità di diversificazione dei servizi di accesso ad Internet in base al livello di qualità garantita, come si andrà ad esplicitare nel prosieguo.

7. Problematiche giuridiche e tecniche: i servizi a qualità garantita possono limitare la neutralità della rete Internet? Un cenno alla tematica negli USA

La problematica relativa alla neutralità della rete con riferimento ai servizi a qualità garantita e le connesse tematiche giuridiche di parità di trattamento non riguardano soltanto l'Europa ed il mercato unico, ma hanno trovato uno sviluppo ed una evoluzione anche in una realtà federale come quella americana, dove questo concetto viene identificato anche con l'apertura della rete stessa: *Internet Openness*.

Nel dicembre 2010 la FCC (*Federal Communications Commission*) ha emanato il c.d. *Open Internet Order*³⁵, che, riguardo agli *Internet Service Providers*, mette in evidenza i tre principi fondamentali che compongono, d'altra parte, la neutralità della rete: trasparenza, divieto di blocco selettivo del traffico, e divieto di discriminazioni irragionevoli. In via esemplificativa, il documento fa anche riferimento al problema della c.d. *pay for priority*, ossia la prassi per cui si fornisce un servizio di accesso a qualità garantita a fronte di un *surplus* di canone³⁶: ebbene, tale prassi non supererebbe il filtro della non irragionevole discriminazione³⁷. In primo luogo, il *pay-for-priority* rappresenterebbe

³⁴ Cfr. capo V, art. 30 della citata proposta di regolamento.

³⁵ L'atto, denominato the Open Internet R&O (*Report & Order*), è stato adottato il 21 dicembre 2010 ed è entrato in vigore il 20 novembre 2011, quasi un anno dopo.

³⁶ Volendo ricostruire i termini del problema dal punto di vista delle forze economiche in gioco, semplificando, sembra che si siano formati due orientamenti. I content providers (soggetti come Google, EBay, Yahoo!) sarebbero a favore della net neutrality, perché, chiaramente, essa consente di veicolare qualunque tipo di contenuto, mentre, viceversa, gli operatori di rete e fornitori di comunicazioni elettroniche (broadband providers: nella realtà americana Comcast, Verizon etc.) si mostrano contrari, perché una volta venuta meno la neutralità della rete in favore della logica del pay-for-priority e dei servizi a qualità garantita, si possono differenziare i profili di accesso alla rete, anche sotto il profilo economico ed ottenere un lucro maggiore.

³⁷ Nel documento sono riportate quattro ragioni e si conclude testualmente: "*In light of each of these concerns, as a general matter, it is unlikely that pay for priority would satisfy the "no unreasonable discrimination" standard*". (Open Internet R&O, cit. p. 17947, trad. it: alla luce di ciascuno di questi punti critici, come criterio generale, è improbabile che tale prassi di "pagamento-per-priorità" risponderrebbe al requisito standard della non irragionevole discriminazione.

un significativo distacco dalla storia e dalla pratica attuale sulla rete, in secondo luogo, un simile discostarsi da regole cristallizzate da tempo, potrebbe determinare un grave danno all'innovazione ed agli investimenti per la rete e sulla rete Internet, in terzo luogo, gli accordi di *pay-for-priority* potrebbero danneggiare particolarmente gli utenti finali non commerciali, inclusi utenti come blogger, biblioteche, scuole, organizzazioni civiche etc. Infine, in quarto luogo, i fornitori di accesso alla banda larga che cercano di offrire servizi a qualità garantita (attraverso la formula del *pay-for-priority*) sarebbero incentivati a limitare la qualità del servizio fornito agli utenti fuori dal traffico prioritario (*non-prioritized traffic*).

Il dibattito, tuttavia, oggi si arricchisce di ulteriori sviluppi: una recente decisione della Corte d'Appello Federale per il Distretto di Columbia (*Verizon, v. Federal Communications Commission*³⁸) ripercorre i quattro capisaldi del problema (le infrastrutture di rete - *backbone networks* -, i *broadband providers*, i fornitori di *mezzi*³⁹, c.d. *edge providers*, e gli utenti finali - *end users*) e la storia, anche giudiziaria, dell'apertura di Internet. La Corte, però, conclude affermando che, rispetto ai fornitori di accesso alla rete mediante banda larga (i *broadband providers*), pur rimanendo applicabili le regole in materia di trasparenza e *disclosure*, non sono, viceversa, applicabili quelle previste dall'*Open Internet Order* in ordine al divieto di blocchi e di discriminazioni⁴⁰, perché non si tratta di ordinari operatori di rete (*common carriers*)⁴¹ e rimanda poi alla *Federal Communication Commission* per l'adempimento in *ottemperanza* alla decisione.

8. Internet come rete aperta e libera: prospettive critiche

Nonostante la sua complessità, il cuore del principio fondamentale della neutralità della rete è che tutti i contenuti di Internet dovrebbero essere trattati in maniera eguale, e che, di conseguenza, gli operatori di rete non dovrebbero differenziare le modalità di accesso alla rete ed ai servizi (*selective access*) per i propri utenti.⁴²

³⁸ *Verizon, appellante c. Federal Communications Commission*, appellato e *Independent Telephone & Telecommunications Alliance, Et Al.*, Interventuti, nel caso 11-1355 consolidato con 11-1356.

³⁹ La traduzione in questo caso non corrisponde al significato letterale inglese, ma è volutamente riferita al fatto che tali fornitori possano dare accesso sia a servizi, sia a connettività, sia ad applicazioni. Il testo della decisione, sinteticamente, riassume: *Edge providers are those who, like Amazon or Google, provide content, services, and applications over the Internet*. In altri termini, tali *providers* sono coloro che, come Amazon o Google, offrono contenuti, servizi e applicazioni sulla rete. Nella nota 37, *supra*, li abbiamo denominati *content providers*.

⁴⁰ In effetti, la decisione della Corte d'Appello Federale si fonda su una argomentazione tecnico-giuridica per cui la FCC non avrebbe l'autorità per emanare una regolamentazione in questa materia ai sensi del *Communications Act* (Sect. 706). Va, peraltro, evidenziato, come la stessa FCC si sia attivata rapidamente per superare questo ostacolo, introducendo una nuova proposta di regolazione. Cfr. <http://www.nytimes.com/2014/02/20/business/fcc-to-propose-new-rules-on-open-internet.html> (ult.vis. 21/02/2014).

⁴¹ Il fulcro è proprio l'assunto che la connessione a banda larga *non* rientri, per dirla prendendo a prestito le parole del legislatore comunitario, nel servizio universale e dunque non debba essere sottoposta alle regole rigide della missione legate alla natura di servizio pubblico. In ordine a questa problematica, la nuova proposta di regolazione negli Stati Uniti, di cui si fa cenno nella nota precedente, evita di riclassificare direttamente i *providers* di banda larga come operatori di telecomunicazioni, soggetti quindi alle medesime restrizioni, ma piuttosto amplia le garanzie a favore dell'apertura di Internet.

⁴² George S. Benjamin *Internet Content Discrimination: The Need for Specific Net Neutrality Legislation by Congress or the FCC*

Tale differenziazione, per gli operatori di rete e gli ISP (*Internet Service Providers*), si tradurrebbe in regole di gestione del traffico sulla rete (il citato tema del c.d. *traffic management*), ovvero nella possibilità attribuire criteri di priorità ai pacchetti di dati che transitano sulla rete mediante gli strumenti di filtri, blocchi di contenuti, fasce orarie, anche in virtù di accordi diversi con soggetti fornitori di contenuti (es. il fornitore “professionista” e il fornitore “utente”). Metaforicamente parlando, sarebbe come porre dei segnali di “precedenza” rispetto ai pacchetti in transito sulla rete, come nella segnaletica stradale, che ben si attaglia a descrivere il funzionamento dell’infrastruttura di rete, come si è visto per il tema del c.d. *pay-for-priority*.

La differenziata accessibilità alla rete potrebbe portare ad una discriminazione, che determinerebbe una lesione ed una compromissione delle caratteristiche di Internet, su cui ci siamo soffermati già in precedenza (rete aperta e potenzialmente illimitata, e dunque anche neutrale, rispetto a contenuto, mittente, destinatari e tipo di servizio).

La questione centrale, dunque, si riconduce sostanzialmente al più volte ricordato concetto di *neutralità tecnologica*, che ha natura squisitamente giuridica⁴³, come impegno per il legislatore di garantire che nessuna delle diverse tecnologie potenzialmente utilizzabili venga preferita rispetto alle altre, proprio per tutelare la concorrenza nel mercato unico e la libertà di scelta e di accesso dei consumatori/utenti, potenzialmente con qualunque tecnologia.

Il dibattito, peraltro, si estende alla questione se sussista per gli utenti la possibilità di riconoscere un ‘diritto fondamentale’⁴⁴ di accesso ad un *Internet* neutrale o se debba prevalere la garanzia del mercato unico e la tutela della concorrenza, relegando tale diritto ad un livello subordinato.

Il punto è che, allo stato, in assenza di una presa di posizione più netta, la neutralità della rete è, appunto, *tendenziale*, da “tenere nel massimo conto”.

in Light of the Recent Anti Net Neutrality Actions by Comcast Corporation, 2009, Southwestern University Law Review.

⁴³ A partire dal dato testuale: “tenere nel massimo conto”, si potrebbe qualificare la neutralità tecnologica come principio generale, sempre in divenire: la tecnologia è sempre in evoluzione, ma il punto di vista giuridico deve rimanere neutrale, nella massima misura possibile.

⁴⁴ La qualificazione come diritto ‘fondamentale’ fa riferimento alle interessanti questioni sollevate già dall’allora Garante per la protezione dei dati personali, Stefano Rodotà, in occasione della Relazione annuale del 2004 che si riproduce di seguito per la parte che interessa: « Nasce da qui la necessità di riconsiderare alcune fondamentali categorie costituzionali. Il costante riferimento alla necessità di “rispetto dei diritti e delle libertà fondamentali” (art. 2.1 del Codice) non implica soltanto un confronto continuo tra le specifiche forme di trattamento dei dati personali ed i singoli diritti e libertà. Impone ormai una ricostruzione di libertà e diritti aderente all’ambiente tecnologico nel quale vengono esercitati. Non si può sfuggire ad alcune domande: le “formazioni sociali” (art. 2 Cost.) possono essere anche le comunità virtuali create nel cibernazio? Le garanzie della libertà personale (art. 13) devono essere estese anche al corpo “elettronico”, seguendo la traiettoria della rilettura dell’*habeas corpus* come *habeas data*? Qual è la portata della libertà di circolazione (art. 16) in presenza della videosorveglianza e del diffondersi delle tecniche di localizzazione? Regge la distinzione tra dati “esterni” e “interni” delle comunicazioni quando queste si svolgono su *Internet*, modificando i termini in cui deve parlarsi della loro libertà e segretezza (art. 15)? Come si atteggiavano in rete la libertà di associazione (art. 18), la stessa libertà religiosa (art. 19)? Il diritto di manifestare liberamente il proprio pensiero (art. 21) deve essere messo in rapporto con il diritto all’anonimato nelle comunicazioni elettroniche, con il diritto a respingere i controlli sulle proprie relazioni elettroniche (lo abbiamo segnalato in una lettera al Presidente del Senato)? L’accessibilità alla proprietà (art. 42.2), quando si traduce nella libera appropriabilità di determinati beni per via elettronica, secondo una logica dei *commons*, dei beni comuni, deve anche escludere l’identificazione personale dei soggetti che accedono? Se non si procede a questa reinterpretazione e ricostruzione del quadro costituzionale, la sua capacità di garanzia ne risulterebbe gravemente menomata. Verrebbe esclusa, infatti, la tutela della persona proprio nelle situazioni che, oggi, mettono più a rischio la sua libertà e dignità ».

Come negli Stati Uniti, anche in Europa il dibattito è acceso⁴⁵ e la Commissione Europea, proprio con la proposta di regolamento in discussione, vorrebbe introdurre una ulteriore deroga (in via regolamentare e dunque con applicazione immediata e diretta in tutti gli Stati membri) al principio di neutralità (fissato in via di direttiva e dunque di armonizzazione con l'attribuzione che resta in capo ai singoli Stati membri).

Tutto ciò in nome dello sviluppo economico e della tutela della concorrenza, come già era accaduto con riferimento al roaming intracomunitario con l'euro-tariffa ed allo spettro-dati con la transizione alla TV digitale⁴⁶.

Questi problemi sono sia di carattere politico che giuridico.

In ultima istanza, la domanda chiave resta: Internet come rete aperta e libera, alla luce di queste considerazioni, resta tale?

Come deve essere qualificato il diritto di accesso alla rete?

Oggi, forse, le prospettive normative esistenti soltanto apparentemente si possono considerare divergenti: da una parte abbiamo gli Stati Uniti, dove la difesa normativa dell'apertura di *Internet* viene in parte contestata a livello giurisprudenziale introducendo la distinzione tra *provider* ordinari e *broadband provider*, dall'altra, l'Europa sembra, invece, orientata ad introdurre proprio normativamente una deroga alla neutralità, in via regolamentare, e dunque di eccezione, ma pur sempre con applicabilità immediata e diretta su tutto il territorio comunitario. Se tale distinzione interpretativa sia soltanto apparente o corrisponda ad una reale differenza di politica normativa⁴⁷, resta, per il momento, un problema aperto⁴⁸.

⁴⁵ Peraltro, da un punto di vista fattuale, è interessante notare come, secondo uno studio per la Commissione Europea (*Quality of Broadband Services in the EU* di Samkowns) del Marzo 2012, le velocità della banda larga in Europa sono più alte che negli Stati Uniti.

⁴⁶ Cfr. *supra* par. 3.

⁴⁷ Del resto, anche il BEREC, nelle osservazioni alla proposta di regolamento citata, esprime serie preoccupazioni, ritenendo che le proposte rappresentino un sostanziale cambiamento nel rapporto di forza fra la Commissione, da un lato, e gli Stati membri, il BEREC e le autorità nazionali dall'altro, centralizzando la regolamentazione dei mercati nazionali senza adeguata giustificazione.

⁴⁸ V'è però da dire, nel tentativo di tracciare una prospettiva uniforme rispetto alla tutela ed alla gestione della rete, che occorrerebbe ancora riferirsi alle proposte di adozione di un codice mondiale di Internet già, peraltro, sollecitato e proposto dal filosofo Vittorio Frosini. Cfr. V. Frosini, *Serve un codice mondiale (per Internet)*, in «Telèma», n. 8, pp. 72-75, 1997.

LA DEMOCRAZIA ELETTRONICA: ASPETTI TEORICI E METODOLOGICI

Wanda D'Avanzo

 *Multimedia*



Clicca sull'immagine o fotografa il QrCode
per accedere al MediaBook CLIOedu

Buongiorno a tutti. Ringrazio il prof. Limone e l'ANDIG per l'invito a partecipare a questa giornata di studio, così piena di argomenti di grande attualità e di spunti per future riflessioni sul tema delle nuove tecnologie. L'argomento di cui mi occuperò è la democrazia elettronica: tematica assolutamente attuale e nota nello scenario politico nazionale, nonché molto complessa perché legata a problemi teorici relativi ad un ripensamento della democrazia in sé considerata.

Il mio intervento si articolerà su due punti principali: una prima definizione della democrazia elettronica, anche attraverso una breve descrizione degli strumenti tecnologici su cui essa si basa; e, secondariamente, un'analisi, molto semplificata, delle teorie, che sono state elaborate in relazione all'applicazione delle tecnologie informatiche ai processi della politica.

Quando si parla di democrazia elettronica si fa riferimento ad un nuovo spazio di comunicazione aperto dalle reti telematiche costituito da un insieme di strumenti e modelli tecnologici volti ad accrescere la partecipazione dei cittadini ai momenti decisionali dell'azione pubblica, nell'ambito di percorsi di rivitalizzazione della sfera del confronto tra istituzioni pubbliche, rappresentanti politici e cittadini elettori¹.

L'*e-democracy* riguarda, quindi, l'applicazione delle ICT a sostegno della partecipazione dei cittadini ai processi democratici più propriamente politici; di partecipazione alla determinazione delle scelte pubbliche². Lo sviluppo del concetto di democrazia elettronica è strettamente connesso, da un lato, alla cosiddetta *governance*, e, dall'altro, ai processi d'innovazione e di riforma che hanno interessato, negli ultimi anni, il settore pubblico, e hanno ad oggetto, appunto, l'utilizzo delle nuove tecnologie dell'informazione e della comunicazione.

La *governance* rappresenta un nuovo paradigma di gestione della cosa pubblica, all'attenzione del dibattito europeo, che si basa su forme d'interazione e coordinamento dell'azione politica tra stato e società, di coinvolgimento e confronto tra l'opinione pubblica e le istituzioni. La *governance* trova giustificazione nella tendenza al decentramento istituzionale della politica, in una logica che crea le condizioni per l'azione dei diversi attori coinvolti, che possono costruire propri percorsi all'interno della politica stessa, in base ad un approccio partecipativo. La ricerca della *governance* rappresenta la più recente variazione della dottrina di governo, che richiede una maggiore attenzione al coinvolgimento dell'opinione pubblica, mediante il rafforzamento della partecipazione alla vita delle istituzioni, della comunicazione e del dialogo sociale³.

Per quanto riguarda, poi, i processi di riforma del settore pubblico, in Italia, è necessario fare riferimento al Codice dell'Amministrazione Digitale, d.lgs. 82/2005 s.m.i., che, all'art. 9, sancisce il diritto alla partecipazione democratica elettronica: lo stato favorisce ogni forma di uso delle nuove tecnologie per promuovere una maggiore partecipazione dei cittadini al processo democratico e per facilitare l'esercizio dei diritti politici e civili sia individuali che collettivi. L'idea di base della democrazia elettronica è, quindi, quella di ampliare e migliorare, nei mezzi e nei contenuti,

¹ UFFICIO STUDI DEL MINISTRO PER L'INNOVAZIONE E LE TECNOLOGIE, *Rapporto innovazione e tecnologie digitali in Italia*, Istituto Poligrafico e Zecca dello Stato, Roma 2003, pp. 140-145. Per una più ampia trattazione del tema della democrazia elettronica, mi sia consentito un rinvio al mio, W. D'AVANZO, *Partecipazione, democrazia, comunicazione pubblica. Percorsi di innovazione dell'amministrazione digitale*, Rubbettino, Soveria Mannelli 2009.

² A.C. FRESCHI, *La società dei saperi. Reti virtuali e partecipazione sociale*, Carocci, Roma 2002, p. 42.

³ Così H.J. BLANKE, "Government e governance nel ventunesimo secolo. Aspetti giuridici e politici dei nuovi modelli di direzione", in «Teoria del diritto e dello Stato», 1, 2004, p. 113; ed anche S. FADDA, *Governance territoriale e progettazione integrata*, in DEIDDA D. (a cura di), *Governance e sviluppo territoriale*, Formez, Roma 2003, pp. 65-66.

il rapporto cittadino-politica e il processo di deliberazione delle decisioni che riguardano la collettività, aprendo a nuove forme di partecipazione.

Vediamo adesso attraverso quali strumenti tecnologici trova attuazione la democrazia elettronica. Dal punto di vista strutturale, le tecnologie a sostegno della democrazia elettronica si possono distinguere in tre differenti tipologie: tecnologie per l'informazione, per il dialogo e per la consultazione. Tre le prime rientrano, ad esempio, le *newsletters* tematiche: iscrivendosi a una *newsletter* e fornendo il proprio indirizzo *e-mail*, il cittadino sceglie di ricevere notizie su argomenti di suo interesse nella propria *mailbox* personale, in tal modo fornendo all'amministrazione un *feedback* indiretto sui temi più sentiti e la possibilità di quantificare e valutare il grado di interesse per le informazioni e i servizi erogati. Vi sono poi le tecnologie per il dialogo, tra cui sicuramente i *forum* di discussione, i *blogs* e le *mailing lists*, che consentono una comunicazione bidirezionale⁴. Infine, le tecnologie per la consultazione che riguardano, in particolare, il voto elettronico in tutte le sue forme, e di cui parleranno ampiamente i prossimi relatori.

È noto il sempre maggiore ricorso alle nuove tecnologie da parte dei partiti politici. Ma le prime forme di partecipazione e propaganda politica veicolate dal web e le prime reti civiche sono state sperimentate già dal 1995, mutate dai modelli statunitensi⁵.

Orbene, il discorso sulla democrazia elettronica, intesa come utilizzo delle nuove tecnologie per rinnovare e ammodernare gli strumenti della partecipazione, del controllo e del consenso intorno alle decisioni democratiche, introduce una riflessione teorica, di carattere filosofico; una discussione sul potenziale democratico dei nuovi *media* e di Internet in particolare. Il concetto di *e-democracy*, centrato sulla forma politica che una società pervasa dalle tecnologie può assumere, lascia intravedere una possibilità di ripensamento stesso della politica⁶. Si delineano, pertanto, alcuni scenari che prefigurano l'impatto politico delle tecnologie informatiche sulle democrazie contemporanee. Ciò che ci si chiede è se la tecnologia comporti il rischio di degenerare in forme di totalitarismo elettronico oppure se possa favorire la democrazia. Dunque, i due poli su cui, molto schematicamente, si concentra la riflessione sul tema sono: i potenziali rischi contro la democrazia insiti nella rete e i vantaggi che, invece, l'uso delle tecnologie potrà comportare.

C'è chi sostiene, dal primo punto di vista, che l'utilizzo della rete potrebbe portare ad una pericolosa concentrazione del potere nella mani di pochi; diversamente, dal lato opposto, c'è chi sostiene che, gli strumenti informatici e telematici potrebbero creare le condizioni per cancellare

⁴ Dipartimento della funzione pubblica, Linee guida per la promozione della cittadinanza digitale: e-democracy, Supema, Roma 2004, pp. 71 ss.

⁵ In tema di *web politics*, l'esperienza italiana mostra i suoi primi due momenti più significativi durante la campagna elettorale del 2001 e la consultazione delle amministrative e delle regionali del 2005, in cui l'utilizzo della rete ha visto progressi importanti. Una ulteriore vicenda si è registrata durante la prova elettorale del 2006, fino al più attuale e costante ricorso alle tecnologie da parte del Movimento 5 Stelle. Per approfondire le tematiche connesse agli strumenti tecnologici che supportano la democrazia elettronica, si vedano, tra gli altri, D. PITTERI, *Democrazia elettronica*, Laterza, Roma-Bari 2007; P. COSTANZO, "La democrazia elettronica (note minime sulla cd. E-democracy)", in «Diritto dell'Informazione e dell'Informatica», 3, 2003; S. RODOTÀ, *Tecnopolitica*, Laterza, Roma-Bari 2004; PIZZETTI F., *Partiti politici e nuove tecnologie*, XXIII Convegno annuale dell'Associazione Italiana dei Costituzionalisti – *Partiti politici e società civile a sessant'anni dall'entrata in vigore della Costituzione* – Alessandria, 18 ottobre 2008, in *Astrid* (www.astrid-online.it).

⁶ D. Pitteri, op. cit., p. 13.

la rappresentanza e riportare ad una nuova forma di democrazia diretta⁷.

Lo schema che contrappone la democrazia rappresentativa alla democrazia diretta non coglie, però, il vero tratto caratteristico che distingue, da entrambi i modelli, la forma che assume un sistema politico innervato dalle reti digitali. Mentre democrazia rappresentativa e democrazia diretta incarnano una partecipazione intermittente, le nuove tecnologie rendono i cittadini potenziali attori permanenti del processo democratico⁸.

È necessario, quindi, superare questa contrapposizione e aprire a nuove prospettive. E, infatti, nello scenario degli studi politici, sta crescendo il dibattito sul concetto di democrazia deliberativa, proposta come un superamento o, comunque, un completamento della democrazia rappresentativa. Scopo della deliberazione, in questa nuova idea di democrazia, è quello di arrivare a un consenso motivato razionalmente, di trovare delle ragioni persuasive per tutti. La democrazia, in questo modo, apre un processo di discussione pubblica che conduce alla decisione, in cui è indispensabile che ognuno abbia l'opportunità di conoscere e valutare adeguatamente le questioni che devono essere deliberate. La comunità politica si configura, così, come un ambito di condivisione delle regole di discussione e argomentazione, generalmente accettate, in cui è possibile confrontarsi, ragionare e agire⁹.

Quali sono, infine, le criticità legate alla democrazia elettronica. E perché siamo ancora lontani, nonostante gli esperimenti di successo in tal senso, da una democrazia deliberativa, o anche partecipativa. Innanzitutto, perché viene meno l'elemento dell'accesso che è una preconditione della partecipazione, che sta alla base della democrazia elettronica.

Esiste, infatti, ancora oggi, il problema del *digital divide*, cioè di quel fenomeno di esclusione determinato dall'impossibilità di una parte della popolazione ad accedere ed utilizzare le nuove tecnologie. Questo comporta la non linearità del processo di digitalizzazione che ha creato un vistoso iato tra coloro che sono in grado di far uso di questi strumenti, che rappresentano una sorta di *élite* del web, e coloro che, invece, non possono farne uso o non hanno la formazione necessaria per farlo. Il *digital divide* determina una violazione dell'art. 3 Cost. perché crea delle nuove disuguaglianze di fatto; determina, altresì, la violazione dell'art. 9 del codice dell'amministrazione digitale che, seppure sia una norma programmatica, ha espressamente introdotto, nel nostro ordinamento, un preciso diritto alla partecipazione in rete.

Accanto a questo aspetto, ciò che riveste anche particolare importanza è l'educazione della cittadinanza alla democrazia. Solo la ricettività del contesto sociale, infatti, può attualizzare le potenzialità tecniche dei mezzi di comunicazione. La sostanza discorsiva della democrazia può

⁷ A. DI GIOVINE, "Democrazia elettronica: alcune riflessioni", in «Diritto e società», 1, 1995, p. 403; F. DI MASCO, "Democrazia elettronica: insidie, illusioni, prospettive", in «Cyberspazio e diritto», vol. 6, 3, 2005, p. 318. Gli aspetti filosofici della democrazia elettronica sono trattati da N. BOBBIO, *Il futuro della democrazia*, Einaudi, Torino 1995, ed anche da G. ZAGREBELSKY, "Dialogo con il Presidente", in «Micromega», 2, 1995, p. 306. Le tesi favorevoli all'introduzione delle nuove tecnologie per l'allargamento della partecipazione politica e il rafforzamento della democraticità dei regimi politici sono evidenziate, tra gli altri, da G. VATTIMO, *La società trasparente*, Garzanti, Milano 1989 e da R. DAHL, *La democrazia e i suoi critici*, Editori Riuniti, Roma 1990.

⁸ F. DI MASCO, *op. cit.*, pp. 319-320.

⁹ Sulla democrazia deliberativa, cfr. L. CURINI, "Note sulla democrazia deliberativa: giochi, preferenze e consenso", in «Quaderni di scienza politica», 3, 2004, p. 522; J. HABERMAS, *Fatti e norme*, Guerini e Associati, Milano 1996; ID., *Morale, Diritto, Politica*, Einaudi, Torino 2007; ID., *L'inclusione dell'altro*, Feltrinelli, Milano 1998; ID., "Legittimazione in forza dei diritti", in «Fenomenologia e società», 2, 1997.

essere alimentata solo da flussi comunicativi originati da una sfera pubblica autonoma, vigile e attiva, che tenga in vita la libertà comunicativa. La democrazia continua ha bisogno di partecipazione continua¹⁰.

D'Altro canto, però, a mio avviso, non basta l'educazione della cittadinanza, rendendosi necessaria anche un'educazione alla democrazia dei rappresentanti, cioè di coloro che sono chiamati a fare da mediatori, e dunque rivestono un ruolo fondamentale, nel processo di trasformazione del consenso in decisione.

Grazie.

¹⁰ F. DI MASCIO, *op. cit.*, p. 324.

IL VOTO ELETTRONICO: DALL'ESPERIENZA DEL PROGETTO "SALENTO EVOTING" AL PROSSIMO REGOLAMENTO DI VOTO PER GLI ITALIANI RESIDENTI ALL'ESTERO

Marco Mancarella

 *Multimedia*



Clicca sull'immagine o fotografa il QrCode
per accedere al MediaBook CLIOedu

Abstract: Il voto elettronico rappresenta, oggi, una realtà democratica in molti Paesi al mondo, ma non ancora in Italia ove, negli anni, si sono succedute una serie di sperimentazioni nelle Regioni ordinarie e concrete svolte normative in quelle a statuto speciale. L'ultima sperimentazione è stata realizzata nel 2013 nei Comuni pugliesi di Martignano e Melpignano (Progetto "Salento eVoting"), che ha condotto alla realizzazione di un referendum consultivo mediante l'utilizzo dell'urna elettronica dello Stato di Jalisco (Messico), già testata nel 2012 nel paese centroamericano con pieno valore legale del voto espresso. Un punto normativo di svolta in Italia potrà essere rappresentato dall'emanando Regolamento per le elezioni, da parte degli italiani residenti all'estero, dei loro rappresentanti presso i COMITES e il CGIE (v. comma 1, art. 1, D.L. 30 maggio 2012, n. 67, convertito con Legge 23 luglio 2012, n. 118).

Nowadays e-voting is a democratic reality in many Countries of the world, but not yet in Italy, where, over the years, a series of tests were carried out in the ordinary Regions and concret turns in those with a special status. The last test was carried out in 2013 in two towns, in Apulia, Martignano and Melpignano (Project "Salento eVoting"), which led to a consultative referendum through the use of the electronic ballot box coming from the state of Jalisco (Mexico), already tested in 2012 in the Central American country with full legal validity of the vote. A regulatory turning point in Italy will be represented by amending Regulations for the election, by the Italians residing abroad, of their representatives at the COMITES and CGIE (see paragraph 1, art. 1, DL May 30, 2012, n. 67, converted into Law July 23, 2012, n. 118).

Parole chiave: eVoting, iVoting, sicurezza, italiani residenti all'estero.

Sommario: 1. L'ultima sperimentazione di eVoting in Italia: il Progetto "Salento eVoting"- 2. La realizzazione del voto elettronico per gli italiani residenti all'estero - 3. Futuro e prospettive dell'eVoting.

1. L'ultima sperimentazione di eVoting in Italia: il Progetto "Salento eVoting"¹

L'ultima sperimentazione di eVoting in Italia è rappresentata dal Progetto "Salento *eVoting*". Esso nasce dall'esperienza internazionale maturata dai componenti del Laboratorio di ricerca sull'*eGovernment* dell'Università del Salento nel settore del voto elettronico (Messico, Brasile, Francia, Grecia). Il Progetto mira a sviluppare un'intensa attività di ricerca e sperimentazione in tema di voto elettronico in seggi presidiati (*eVoting*)². Non mira, pertanto, allo studio di sistemi digitali di voto

¹ Il presente contributo riassume i contenuti dell'intervento effettuato nell'ambito del Seminario di studio "La Circoscrizione estero e la riforma del voto all'estero", organizzato il 3 luglio 2014 presso la Camera dei Deputati da Angela Fucina Nissoli (deputata eletta nella circoscrizione America settentrionale e centrale), in collaborazione con Gianni Lattanzio (Associazione "Dialoghi" di Roma) ed è tratto dal testo: M. Mancarella, *eVoting e nuove dimensioni della democrazia*, Trento, Tangram Edizioni Scientifiche, 2013.

² In base alle Linee Guida sul voto elettronico del Consiglio d'Europa del 2004, Rec(2004)11, per "*eVoting*" occorre intendere: "Il ricorso a mezzi elettronici, almeno al momento dell'operazione di voto propriamente detta, nell'ambito di un'elezione o di un *referendum*". Per "*remote eVoting*", anche detto "voto a distanza", invece: "Il voto elettronico in

che comportino maggiori problematiche di compatibilità con il dettato dell'art. 48 Cost., come il voto da remoto tramite *Internet (iVoting)*.

Il Progetto prevede l'utilizzo nella Provincia di Lecce, in una o più tornate elettorali o referendarie, dell'urna elettronica messicana (giunta oggi alla quinta generazione), già testata nel Paese centro-americano alle elezioni dell'1 luglio 2012. La sperimentazione deve poi condurre alla progettazione e realizzazione di un prototipo di urna elettronica usabile in Italia e, se adeguatamente implementata e rispondente agli *standard* internazionali, anche in altri Paesi europei.

Il Progetto si contraddistingue nel panorama internazionale in quanto primo caso di ricerca e trasferimento intercontinentale di *know-how*, tecnologico e organizzativo, tra Enti pubblici (IEPC Jalisco da un lato ed i Comuni salentini di Martignano e Melpignano dall'altra) nel settore *eVoting*. Il primo *step* istituzionale, che ha poi condotto ad un Protocollo d'intesa internazionale Italia – Messico, si è avuto in data 4 dicembre 2012, con la sottoscrizione di una Dichiarazione di interesse da parte della Provincia di Lecce, del Dipartimento di Storia, Società e Studi sull'Uomo – Laboratorio di *eGovernment* dell'Università del Salento, dell'Istituto Electoral y de Participacion Ciudadana del Estado de Jalisco (Messico), della Clio S.p.a., del Comune di Martignano, del Comune di Melpignano e dell'Unione dei Comuni della Grecia Salentina. Al momento della sottoscrizione si è anche proceduto ad una sperimentazione del voto elettronico in aula consiliare del Palazzo dei Celestini della Provincia di Lecce da parte del Presidente Antonio Gabellone.

Successivamente alla Dichiarazione, il Prefetto di Lecce Giuliana Perrotta, ricevuto il nulla osta del Ministero degli Interni (n. prot. 4829 del 29 novembre 2012) convocava in data 11 dicembre

cui l'operazione di voto propriamente detta è realizzata tramite un dispositivo non controllato da un funzionario elettorale”.

Dal contenuto delle Linee Guida emerge una certezza, importante nel districarsi nelle molteplici forme di voto elettronico: ogni sistema informatico e telematico di voto rientra nell'*eVoting*, con previsione poi di un sotto-insieme rappresentato dal “*remote eVoting*”. Da ciò consegue che, in linea generale, ogni tipologia di voto elettronico che nel prosieguo esamineremo, rientra sempre nella definizione di “*eVoting*”, poi specificandosi ulteriormente in base ad una serie di elementi distintivi.

Le classificazioni essenziali tra le varie forme di voto elettronico non possono, dunque, che partire da queste prime due definizioni. Chiarita la distinzione di fondo tra i due insiemi (il macro-insieme “*eVoting*” e il sotto-insieme “*remote eVoting*”), si rende ora necessario approfondire le varie ulteriori declinazioni possibili dell'*eVoting*. Occorre subito precisare che quando si parla delle nuove frontiere della democrazia elettronica, e nello specifico dell'*eVoting*, si tende a confondere quattro diversi livelli, caratterizzati dall'utilizzo di sistemi di registrazione/invio del voto differenti:

- a) il “voto elettronico semplice”, vale a dire quello espresso tramite un *computer* che, però, viene installato in un seggio e non è connesso alla Rete *Internet* (anche detto voto “in loco”);
- b) il “voto *online*” vero e proprio, che si esprime usando la Rete *Internet (Internet Voting - iVoting)*, a prescindere dal luogo da cui ci si collega;
- c) il “voto tramite dispositivi mobili” (*mobile Voting - mVoting*), ovvero la frontiera più avanzata del voto elettronico, in quanto è possibile utilizzare il telefono cellulare;
- d) il “voto tramite il telecomando” di una televisione interattiva o digitale.

L'*iVoting*, l'*mVoting* e il voto tramite televisione rappresentano tendenzialmente forme di voto “non presidiato”, poiché la preferenza è espressa a distanza in assenza di un pubblico ufficiale/funzionario elettorale. Ma questa non è una regola assoluta. Si consideri, ad esempio, la possibilità che l'*iVoting* sia utilizzato in un seggio presidiato: il votante, pertanto, esercita il suo diritto tramite terminale alla presenza del funzionario pubblico e il voto viaggia immediatamente in Rete per essere registrato su un *server* in remoto.

Normalmente l'*iVoting* viene anche definito “*home voting*”, in quanto associato alla possibilità di esercitare il diritto di voto anche dalla propria dimora: ma una tale definizione, sebbene ricorrente, a parere di chi scrive è fuorviante, in quanto anche l'*mVoting* e il voto tramite televisione potrebbero essere definiti, a ragione, modalità di “*home voting*”.

Nelle varie esperienze internazionali, il voto elettronico semplice rappresenta il modello prevalente.

2012 gli Enti interessati per la sottoscrizione di un Protocollo internazionale, finalizzato all'avvio del Progetto "Salento *eVoting*". L'intero progetto trova quindi legittimazione internazionale con il Protocollo d'intesa, sottoscritto tra i seguenti partner: Dipartimento di Storia, Società e Studi sull'Uomo - Laboratorio di *eGovernment* dell'Università del Salento, Dipartimento di Studi Umanistici dell'Università di Foggia, Prefettura di Lecce, Instituto Electoral y de Participacion Ciudadana del Estado de Jalisco (Messico), Clio S.p.a., Comune di Martignano, Comune di Melpignano, Unione dei Comuni della Grecia Salentina³.

Successivamente alla sottoscrizione di tale protocollo sono state effettuate molteplici attività:

- i Comuni interessati, Martignano (1.770 abitanti) e Melpignano (2.242 abitanti), hanno approvato un "Regolamento comunale per la disciplina del *referendum* consultivo" e deliberato l'indizione di quest'ultimo con modalità informatiche, sottoponendo alle popolazioni il seguente quesito in accordo con la Prefettura di Lecce: "Vuoi tu la fusione del tuo comune di residenza con altri comuni aventi popolazione fino a 5.000 abitanti?";
- è stato realizzato un sito *Internet* dedicato al Progetto (www.salentoevoting.it), costantemente implementato e che potrà essere utilizzato anche per la seconda fase della sperimentazione, destinata alla realizzazione di *test eVoting* su più larga scala;
- ogni informazione inerente gli studi e la prima sperimentazione è stata veicolata sui *social network* e *media* telematici più comunemente utilizzati (Facebook, Twitter, Youtube), nonché sui *mass media* tradizionali⁴;
- è stato costituito un gruppo di ricerca, composto da tre docenti dell'Università del Salento, che ha predisposto nel mese di marzo 2013 una Proposta di Risoluzione sul voto elettronico al Parlamento Europeo, il tutto su specifica richiesta da parte del Vice Presidente del Parlamento Europeo Gianni Pittella⁵;
- sono state realizzate attività divulgative e di approfondimento sul tema del voto elettronico presso i Comuni coinvolti nella sperimentazione (*Info Day* e Seminari tematici);
- sono stati nominati i seguenti Osservatori internazionali per la sperimentazione: Robert Etien (Università di Parigi XIII - Francia), Jordi Barrat (Universitat Rovira i Virgili de Tarragona - Spagna), Rodrigo Aguilar Benignos (AKA Consulting Washington DC - USA), José Tomas Figueroa Padilla (IEPC Jalisco – Messico), Victor Hugo Bernal Hernandez (IEPC Jalisco – Messico).
- con il supporto di un *team* di ingegneri dell'IEPC Jalisco, coordinati da Ramiro Feliciano Garzón Contreras, e in sinergia con quello del partner progettuale Clio spa, coordinato dal General Manager Gabriele Conte, si è proceduto alla reingegnerizzazione dei processi *software* dell'urna elettronica messicana, al fine di porli a norma con l'ordinamento elettorale italiano sotto i seguenti profili: possibilità di scheda bianca⁶; traduzione dalla lingua spagnola a quella

³ Il Protocollo ha individuato chi scrive quale Responsabile scientifico di Progetto. Per maggiori delucidazioni si rinvia all'URL: <http://www.salentoevoting.it/it/la-firma-del-protocollo-ufficiale-%C3%A8-arrivato-il-gran-giorno>, consultato nel mese di maggio 2013.

⁴ Si veda la *press room* di Progetto disponibile all'URL: <http://www.salentoevoting.it/it/press-room>, consultato nel mese di maggio 2013.

⁵ La proposta di Risoluzione al Parlamento Europeo è visionabile all'URL: <http://www.salentoevoting.it/it/risoluzione-ue>, consultato nel mese di marzo 2013.

⁶ Il gruppo di ricerca del progetto ha inteso assicurare la possibilità dell'elettore di optare per una scheda bianca, nel

italiana di ogni testo a video e dei verbali stampati dalla macchina in fase di attivazione e chiusura; memorizzazione dei messaggi sonori in lingua italiana utili ai non vedenti per l'ottimale utilizzo del macchinario⁷; rilascio a video, ad orari prestabiliti, del dato di affluenza alle urne. Il referendum consultivo con modalità elettroniche, in totale assenza di schede elettorali cartacee, si è svolto in data 5 Maggio 2013, senza alcuna problematica di gestione delle attività nei seggi e di scrutinio. Nello specifico della sperimentazione in Italia, il dato elettorale elettronico è transitato in totale sicurezza alla chiusura delle urne nel Sistema Pubblico di Connettività, come consentito dal coinvolgimento, nel Protocollo firmato nel dicembre 2012, della concessionaria Puglia del Sistema Pubblico di Connettività, Clio spa. Il mancato utilizzo di schede cartacee può essere visto come un concreto esempio di superamento della classica “informatica parallela”, fase nella quale ci troviamo da circa un ventennio e che tarda a divenire di “informatica pura”.

La sperimentazione ha comportato la totale digitalizzazione delle seguenti fasi:

- espressione del voto;
- spoglio dei voti;
- redazione di tabelle di scrutinio/conteggio dei voti;
- redazione dei verbali;
- trasmissione dei dati ad un server centrale.

Le uniche due fasi non digitalizzate sono state:

- identificazione del votante;
- verifica del diritto di voto.

La mancata digitalizzazione di queste fasi è connessa solo alle odierne funzionalità del macchinario messicano utilizzato. Il Progetto “Salento *eVoting*”, come detto, giunto a regime comporterà la realizzazione di un prototipo in grado di superare anche tali ultime barriere e di identificare l'elettore che utilizza adeguati strumenti elettronici di riconoscimento (ad esempio, carta di identità elettronica).

Nella giornata successiva alla sperimentazione, è stato realizzato in Lecce un convegno internazionale conclusivo, dal titolo “*eDemocracy and eVoting: from the international experiences to the Salento eVoting project*”, con relatori gli osservatori internazionali e alla presenza di rappresentanti istituzionali italiani, al fine di discutere le risultanze della prima fase dell'attività di sperimentazione in un'ottica comparativa con altre esperienze estere. Nel convegno sono stati anche comunicati i dati elettorali, già conosciuti nella loro interezza pochi istanti dopo la chiusura dei seggi e consultabili immediatamente dai cittadini, anche su dispositivi mobili, tramite una piattaforma dedicata *online*. Terminata la prima sperimentazione, il Progetto “Salento *eVoting*” è stato portato all'attenzione della Tavola rotonda “*Digital Democracy Leaders*” del 18 giugno 2013 presso il Parlamento Europeo

rispetto dei principi dettati dalle citate Linee Guida sul voto elettronico del Consiglio d'Europa del 2004. Convinti delle medesime necessità di tutela del diritto di esprimere il proprio voto anche con scheda bianca in modalità elettronica: A. SARAI, *Democrazia e tecnologie. Il voto elettronico*, Bologna, Esculapio, 2008, pp. 34-35; E. Bettinelli, *La lunga marcia del voto elettronico in Italia*, in “Quaderni dell'osservatorio elettorale”, 46, 2002, pp. 5-48.

⁷ I particolari strumenti di ausilio ai portatori di *handicap* permessi dal macchinario messicano vengono incontro e superano la stessa norma contenuta nell'art. 55 del DPR 30 marzo 1957, n. 361, in base alla quale tali possibili elettori, dotati di certificato medico, possono farsi assistere nelle operazioni di voto da persona di fiducia, che può anche esprimere il voto in loro vece. Gli ausili audio-video e tattili dell'urna utilizzata nel Progetto hanno reso superflua l'assistenza al portatore di *handicap* in fase di voto.

di Bruxelles, incentrata sulla “*Digital Citizenship*”, che ha visto il coinvolgimento di un gruppo di giovani esperti e studiosi europei nel settore dell’innovazione e della comunicazione digitale⁸. Il 3 luglio 2013 la discussione sul voto elettronico è continuata nell’ambito del Seminario di studio “La Circoscrizione estero e la riforma del voto all’estero”, organizzato presso la Camera dei Deputati da Angela Fucsia Nissoli (deputata eletta nella circoscrizione America settentrionale e centrale), in collaborazione con Gianni Lattanzio (Associazione “Dialoghi” di Roma). A conclusione dell’incontro, Nissoli, i relatori e gli esperti presenti in platea hanno concordato sulla necessità di organizzare una sperimentazione di voto elettronico, sul modello di quella effettuata nel Salento in data 5 maggio 2013, eventualmente nella Circoscrizione Nord-America.

Prossimo *step* del Progetto “Salento *eVoting*” consiste nell’avvio delle attività di pianificazione, congiuntamente alla Prefettura di Lecce e al Ministero degli Interni, di una possibile seconda fase di sperimentazione del voto elettronico in ambienti presidiati, con pieno valore legale, durante le elezioni europee dell’anno 2014. A tal fine, il Comune di Lecce, nella persona dell’Assessore all’Innovazione tecnologica Alessandro Delli Noci, ha già espresso la disponibilità dell’Ente ad ospitare in alcuni suoi seggi le urne elettroniche.

2. La realizzazione del voto elettronico per gli italiani residenti all’estero

Per comprendere al meglio il prossimo futuro *eVoting* dei processi elettivi coinvolgenti gli italiani residenti all’estero, occorre innanzitutto capire la genesi e peculiare struttura del sistema elettorale che li riguarda.

Gli italiani residenti all’estero votano in base ad una serie di normative oggi in vigore ma che, in questa fase storica, sono oggetto di discussione e sulla via di una notevole rivisitazione ad opera del Legislatore, nell’ottica di una più complessiva riforma istituzionale.

Il diritto di voto per i residenti all’estero è stato introdotto nel nostro ordinamento con Legge costituzionale 17 gennaio 2000, n. 1, “Modifica all’articolo 48 della Costituzione concernente l’istituzione della circoscrizione Estero per l’esercizio del diritto di voto dei cittadini italiani residenti all’estero”. La Legge inserisce all’art. 48 della Costituzione, dopo il secondo comma, il seguente inciso: “La legge stabilisce requisiti e modalità per l’esercizio del diritto di voto dei cittadini residenti all’estero e ne assicura l’effettività. A tale fine è istituita una circoscrizione Estero per l’elezione delle Camere, alla quale sono assegnati seggi nel numero stabilito da norma costituzionale e secondo criteri determinati dalla legge”.

Con successiva Legge Costituzionale 23 gennaio 2001, n. 1, “Modifiche agli articoli 56 e 57 della Costituzione concernenti il numero di deputati e senatori in rappresentanza degli italiani all’estero”, si è completato il quadro di riforma del voto dei residenti all’estero, rimasto virtuale per la mancata contestuale modifica nel 2000 di tutti gli articoli della Costituzione interessati (artt. 48,

⁸ Per un approfondimento in ordine ai lavori e interventi della Tavola rotonda, si rinvia all’URL: <http://www.salentoevoting.it/it/digital-democracy-leaders-bruxelles>, consultato nel mese di giugno 2013.

56 e 57). Con la Legge Costituzionale n. 1/2001 sono stati definiti, quindi, il numero di senatori e deputati da eleggere nella circoscrizione Estero.

La circoscrizione Estero è suddivisa in quattro ripartizioni (Europa, compresi i territori asiatici della Federazione russa e della Turchia; America meridionale; America settentrionale e centrale; Africa, Asia, Oceania e Antartide) in ciascuna delle quali è eletto almeno un senatore e un deputato, mentre gli altri due seggi per il Senato e gli altri otto per la Camera sono distribuiti tra le stesse ripartizioni in proporzione al numero dei cittadini che vi risiedono.

La procedura ordinaria di voto è quella per corrispondenza presso l'abitazione degli elettori residenti all'estero⁹. La modalità di voto per corrispondenza è possibile solo in quegli Stati con i quali il Governo italiano ha concluso apposite intese, pubblicate *online* sul sito *Web* del Ministero degli Esteri in ogni tornata elettorale. Per i rimanenti Stati, il residente all'estero deve necessariamente rientrare in Italia per esercitare il diritto di voto. Le schede votate dagli elettori all'estero, incluse nelle apposite buste pervenute per corrispondenza agli Uffici consolari, vengono spedite in Italia attraverso gli stessi Consolati mediante valigia diplomatica accompagnata. I plichi arrivati in Italia vengono presi in consegna dall'Ufficio centrale per la circoscrizione Estero che provvede al riepilogo dei risultati ufficiali delle sezioni, nonché al riparto e alla assegnazione dei seggi con sistema proporzionale per ciascuna ripartizione e alle corrispondenti proclamazioni.

I cittadini italiani residenti all'estero e regolarmente iscritti all'Anagrafe degli Italiani Residenti all'Estero (AIRE)¹⁰ possono esercitare il diritto di voto all'estero nel luogo di residenza per le ele-

⁹ Per quanto attiene le precise modalità di voto, gli Uffici consolari, spediscono al domicilio di tutti gli elettori, non oltre diciotto giorni prima della data stabilita per le votazioni in Italia, un plico contenente:

- il certificato elettorale;
- la scheda (se elettore della sola Camera o se il voto si esprime per un solo *referendum*) o le schede elettorali (se elettore della Camera e del Senato o se il voto si esprime per più *referendum*) e la relativa busta piccola, nonché una busta affrancata recante l'indirizzo dell'Ufficio consolare competente;
- le liste dei candidati nella ripartizione d'appartenenza;
- un foglio esplicativo delle modalità di voto.

L'elettore:

- esprime il proprio voto sulla scheda o sulle schede elettorali: il voto si esprime tracciando un solo segno sul simbolo della lista prescelta o comunque all'interno del rettangolo che lo contiene, mentre per il *referendum* il voto è espresso tracciando un segno sulla risposta prescelta dall'elettore e, comunque, nel rettangolo che la contiene; l'elettore può, inoltre, per le elezioni politiche, esprimere due voti di preferenza nelle ripartizioni geografiche alle quali sono assegnati due o più deputati o senatori e un voto di preferenza nelle altre ripartizioni;
- deve introdurre la scheda o le schede nella relativa busta piccola e chiuderla;
- deve, inoltre, introdurre la busta piccola nella busta affrancata, unitamente al tagliando staccato dal certificato elettorale comprovante l'esercizio del diritto di voto;
- deve, infine, spedire il tutto entro dieci giorni prima della data stabilita per le votazioni in Italia al Consolato competente. Saranno considerate valide le buste pervenute al Consolato entro le ore 16, ora locale, del giovedì antecedente la data stabilita per le votazioni in Italia (art. 12, comma 7, della Legge n. 459/2001).

Gli elettori residenti all'estero che, entro quattordici giorni dalla data delle votazioni in Italia, non abbiano ricevuto a casa il plico con tutta la documentazione elettorale, possono farne richiesta presentandosi di persona al proprio Consolato.

Per un maggiore approfondimento si rinvia al sito istituzionale del Ministero dell'Interno, visionabile all'URL: <http://www.interno.gov.it/mininterno/export/sites/default/it/temi/elezioni/sottotema006.html>, consultato nel mese di aprile 2013.

¹⁰ L'Anagrafe degli Italiani Residenti all'Estero (AIRE) è stata istituita con Legge 27 ottobre 1988, n. 470, e contiene i dati dei cittadini italiani che risiedono all'estero per un periodo superiore ai dodici mesi, nonché quelli che già vi risiedono, sia perché nati all'estero che per successivo acquisto della cittadinanza italiana a qualsiasi titolo. Essa è gestita dai Comuni sulla base dei dati e delle informazioni provenienti dalle Rappresentanze consolari all'estero e il

zioni politiche nazionali, per i *referendum* abrogativi e costituzionali in base agli artt. 75 e 138 della Costituzione e per le elezioni del Parlamento europeo, con talune differenziazioni.

Il voto all'estero per le elezioni politiche nazionali e i *referendum* è regolato dalla Legge 27 dicembre 2001, n. 459, e dal relativo Regolamento attuativo (DPR 2 aprile 2003, n. 104), in attuazione degli artt. 48, 56 e 57 della Costituzione, che, come detto, hanno istituito la Circoscrizione Estero.

Il voto all'estero per l'elezione dei rappresentanti italiani al Parlamento europeo è invece regolato dalla Legge 24 gennaio 1979, n. 18, e dal DL 24 giugno 1994, n. 408, (convertito in Legge 3 agosto 1994, n. 483).

Terminata la necessaria premessa volta a chiarire genesi e odierna struttura del sistema di voto per gli italiani all'estero, un'attenzione particolare occorre riservarla ai Comitati degli italiani all'estero (COMITES), poiché organismi sui cui processi elettivi, come vedremo nel paragrafo, verrà avviata a breve una reale attività di innovazione tecnologica.

Gli elettori italiani residenti all'estero e regolarmente iscritti all'AIRE possono votare per l'elezione dei rappresentanti dei COMITES (oggi disciplinata dalla Legge 23 ottobre 2003, n. 286 e dal suo regolamento attuativo contenuto nel DPR 29 dicembre 2003, n. 395). I COMITES sono organismi istituiti nel 1985 al fine di rappresentare la collettività italiana, per tali ragioni eletti direttamente dai connazionali residenti fuori dall'Italia. La loro "*mission*" è particolarmente ampia, in quanto include anche attività di studio e ricerca al fine di individuare le esigenze di sviluppo sociale, culturale e civile della comunità di riferimento. Essi promuovono, inoltre, la collaborazione con l'autorità consolare, con le regioni e con le autonomie locali, nonché con enti, associazioni e comitati operanti nell'ambito della circoscrizione consolare, opportune iniziative nelle materie attinenti alla vita sociale e culturale, con particolare riguardo alla partecipazione dei giovani, alle pari opportunità, all'assistenza sociale e scolastica, alla formazione professionale, al settore ricreativo, allo sport e al tempo libero (art. 2 della Legge n. 286/2003).

Operano al momento 124 COMITES diffusi in 38 Paesi: di questi, 67 si trovano in Europa, 23 in America latina, 4 in America centrale, 16 in Nord America, 7 in Asia e Oceania e 7 in Africa.

Al di là del loro considerevole numero, l'importanza dei COMITES è connessa al rapporto con un altro organismo di rappresentanza degli italiani all'estero: il Consiglio Generale degli Italiani all'Estero (CGIE), istituito con Legge 6 novembre 1989, n. 368, (modificata dalla Legge 18 giugno 1998, n. 198) e disciplinato dal regolamento attuativo di cui al DPR 14 settembre 1998, n. 329. Il CGIE, presieduto dal Ministro degli Affari esteri, è organo di consulenza del Governo e del Parlamento sui grandi temi di interesse per gli italiani all'estero e deriva la sua legittimità rappresentativa dall'elezione diretta da parte dei componenti dei COMITES.

I componenti oggi in carica dei COMITES, come quelli del CGIE, sono stati eletti nel 2004. Il mandato ha una durata, teoricamente e in mancanza di proroghe, di cinque anni¹¹.

Compreso il ruolo dei COMITES e CGIE ai fini della rappresentanza degli italiani residenti all'e-

suo aggiornamento dipende dal cittadino, il quale deve tempestivamente comunicare all'ufficio consolare eventuali modifiche del proprio *status*.

L'iscrizione all'AIRE è un diritto-dovere del cittadino (art. 6, Legge n. 470/1988) e costituisce il presupposto per usufruire di una serie di servizi forniti dalle Rappresentanze consolari all'estero, nonché per l'esercizio di importanti diritti.

¹¹ Ad oggi non è ancora avvenuta una nuova elezione dei COMITES e CGIE, rinviata tre volte.

stero, occorre ora meglio comprendere la loro importanza ai fini del voto elettronico.

Le elezioni dei COMITES e CGIE costituiscono ad oggi in Italia l'unico caso in cui la Legge permetta l'utilizzo di strumentazione informatica ai fini del voto¹².

Il comma 1 dell'art. 1 del recente DL 30 maggio 2012, n. 67, convertito con Legge 23 luglio 2012, n. 118, dopo aver individuato come termine massimo per svolgere le prossime elezioni dei COMITES e CGIE la fine dell'anno 2014, così dispone: "Con regolamento da adottare ai sensi dell'articolo 17, comma 2, della Legge 23 agosto 1988, n. 400, e successive modificazioni, entro sei mesi dalla data di entrata in vigore della legge di conversione del presente decreto, su proposta del Ministro degli affari esteri, di concerto con il Ministro dell'economia e delle finanze e con il Ministro delegato all'innovazione tecnologica e allo sviluppo della società dell'informazione, sono stabilite le modalità di votazione e scrutinio nei seggi costituiti presso la sede dell'ufficio consolare o, ove possibile, anche in altri locali predisposti dal comitato elettorale, tenuto conto del numero degli elettori, della loro dislocazione e della disponibilità di personale, anche mediante l'utilizzo di tecnologia informatica, nel rispetto dei principi di personalità e segretezza del voto, in modo da garantire che il relativo onere non superi il tetto di spesa indicato al comma 3 del presente articolo [due milioni di euro], che il sistema di voto con tecnologia informatica sia sicuro da attacchi deliberati o comunque non autorizzati, garantisca il funzionamento del voto da qualunque inefficienza del materiale o del programma tecnologico e consenta all'elettore di poter ottenere conferma del suo voto. Con il medesimo regolamento è stabilita la disciplina delle operazioni di scrutinio nel rispetto del principio di segretezza del voto, adeguate all'adozione del sistema di votazione mediante l'utilizzo di tecnologia informatica, nonché la modalità di partecipazione al voto con tecnologia informatica mediante la disponibilità di postazioni di accesso per gli elettori che non dispongono di un *personal computer* ovvero che si trovano in Paesi in cui la trasmissione cifrata dei dati è interdetta o impossibile".

Tenuto conto della volontà normativa di consentire il voto "anche mediante l'utilizzo di tecnologia informatica", è lecito affermare che il Legislatore abbia superato *de facto* in ambito *eVoting* ogni problematica connessa al bilanciamento tra il principio di effettività ed il principio di segretezza del voto, bilanciamento conclusosi a favore dell'effettività del voto nel caso del voto per corrispondenza introdotto con la citata Legge n. 459/2001.

Nel caso del voto elettronico per i COMITES e CGIE il problema della segretezza del voto è stato probabilmente ritenuto come estremamente limitato nel caso di uso di adeguate tecnologie, diversamente non sarebbe comprensibile l'adozione dell'*eVoting* nel DL n. 67/2012.

Il problema ora si concentra sull'individuazione delle tecnologie adatte e sulla realizzazione di un approfondito studio dei processi di identificazione telematica e gestione sicura del dato elettorale, oltre alla necessaria pianificazione di una totale reingegnerizzazione dei processi amministrativi sottesi all'attività elettorale. Si consideri, peraltro, che l'utilizzo di strumenti elettronici di voto anche per la fase di identificazione dell'elettore comporterebbe materialmente il superamento di un primo, importante, problema di segretezza connesso al "tracciamento" di "comportamenti

¹² Per una più ampia ricostruzione, rispetto al presente paragrafo, delle varie problematiche sottese al voto elettronico degli italiani all'estero, si rinvia a: L. TRUCCO, *Le nuove tecnologie salveranno il voto all'estero degli italiani?*, in "Forum di Quaderni costituzionali", 6 gennaio 2013, p. 9, disponibile all'URL: http://www.forumcostituzionale.it/site/images/stories/pdf/documenti_forum/paper/0387_trucco.pdf, consultato nel mese di aprile 2013.

elettorali” sulla tessera personale del votante. Infatti, l’apposizione su tale tessera di timbri da parte delle sezioni elettorali ad ogni consultazione elettorale comporta “una palese violazione del diritto alla riservatezza del cittadino e della tutela della segretezza non solo del voto, ma più in generale di ogni comportamento elettorale”¹³. Al contrario, iniziare ad utilizzare strumenti informatici e telematici anonimizzanti il dato personale comporterebbe un possibile recupero di legalità.

Volendo elencare i caratteri che il voto elettronico deve rivestire in base al citato art. 1, comma 1, del DL n. 67/2012:

- il sistema informatico deve rispettare i principi di personalità e segretezza del voto;
- il sistema informatico deve essere sicuro in relazione ad eventuali attacchi deliberati o comunque non autorizzati;
- il sistema informatico deve garantire il funzionamento del voto da qualunque inefficienza del materiale o del programma tecnologico;
- il sistema informatico deve consentire all’elettore di poter ottenere conferma del suo voto;
- il sistema informatico deve assicurare il rispetto del principio di segretezza nell’esperimento delle operazioni di scrutinio, che devono essere adeguate rispetto all’adozione del sistema stesso;
- al fine di evitare casi di “divario digitale” (*digital divide*) e, quindi, per permettere una piena partecipazione al voto elettronico degli aventi diritto (*eInclusion*), devono essere sempre rese disponibili postazioni di accesso per gli elettori che non dispongono di un *personal computer* ovvero che si trovano in Paesi in cui la trasmissione cifrata dei dati è interdetta o impossibile.

L’ultimo inciso, inerente le modalità di voto utili ad evitare casi di *digital divide*, denota in sé una decisione chiara, e preventiva rispetto al Regolamento, da parte del Legislatore in ordine alla tipologia di *hardware* e *software* da utilizzare per l’elezione elettronica dei componenti dei COMITES e CGIE: tecnologia *iVoting* in linea generale, sia con modalità “*home voting*” che, in maniera residuale, con postazioni telematiche in seggi presidiate.

Adottando soluzioni *iVoting* per il voto degli italiani residenti all’estero (anche se limitato ai COMITES e CGIE e non per elezioni di altra natura) l’Italia si metterebbe al passo con altre esperienze similari, come ad esempio la votazione popolare federale svizzera del 9 giugno 2013.

La conferma della volontà di procedere lungo la strada di un sistema *eVoting* misto (in larga parte *iVoting* non presidiato, in parte residuale *iVoting* presidiato) viene anche dalle anticipazioni inerenti al testo del Regolamento, ancora in fase di approvazione¹⁴.

Per quanto riguarda le elezioni per il rinnovo di COMITES e CGIE il Ministero per gli Affari Esteri (MAE) ha elaborato una prima bozza di regolamento che modifica le modalità di elezione dei COMITES, in esecuzione dell’obbligo previsto dalla Legge 23 luglio 2012, n.118.

Il progetto di regolamento consegue ad uno studio di fattibilità tecnica e prevede il voto via *Internet*

¹³ A. SARAI, *Democrazia e tecnologie. Il voto elettronico*, cit., p. 40. L’Autore richiama anche il contenuto del Parere del 17 novembre 1999 del Garante per la protezione dei dati personali, nel quale tale organo di garanzia sottolineava come la tessera elettorale permanente fosse da considerarsi uno strumento idoneo a rivelare il comportamento elettorale del soggetto e, in caso di *referendum*, potesse addirittura divenire indicativo dell’orientamento politico.

¹⁴ Si citano nel testo le dichiarazioni del 9 maggio 2013 dell’Ambasciatore Cristina Ravaglia, Direttore generale per gli italiani all’estero e le politiche migratorie, nella relazione svolta al Comitato di Presidenza del CGIE, riunito alla Farnesina. Le dichiarazioni sono disponibili all’URL: http://www.consbahia blanca.esteri.it/Consolato_BahiaBlanca/Archivio_News/Ravaglia+CGIE.htm, consultato nel mese di giugno 2013.

sia in seggi presso gli Uffici consolari sia in remoto, previa distribuzione personale per questa seconda modalità di appositi “PIN” (sola condizione che possa garantire che le credenziali di accesso al sistema *online* siano in possesso del titolare).

Il voto elettronico dovrebbe rispettare le seguenti modalità:

- distribuzione di credenziali per il voto da remoto, valide per tutte le successive consultazioni, al connazionale che ne faccia richiesta, in due tempi: una prima parte consegnata personalmente allo sportello consolare ed una seconda per via telematica;
- attivazione delle credenziali in occasione dell’indizione delle elezioni e previa verifica della qualità di elettore (tramite confronto con l’elenco provvisorio fornito dal Ministero dell’Interno);
- costituzione di seggi presso gli uffici consolari di I categoria¹⁵, con modalità elettronica, tramite apposito applicativo informatico della Rete Internazionale per le Pubbliche Amministrazioni (RIPA)¹⁶;
- possibile costituzione di seggi presso gli uffici consolari di II categoria, dove si voterebbe con modalità analoghe a quelle “da remoto”, (mancando la connessione in RIPA);
- voto da remoto con collegamento da qualsiasi *computer* ad un sito dedicato;
- ricezione e custodia dei voti espressi presso un unico *server* centrale a Roma;
- verifica dei risultati in via elettronica da parte del seggio mediante consultazione della banca dati centrale.

Una particolare criticità nel tradurre in realtà il voto elettronico prospettato dal comma 1, art. 1, del DL n. 67/2012 è connessa alla scarsa dotazione finanziaria (due milioni di euro) a fronte del numero dei seggi da creare. Scarsità di risorse che probabilmente porterà a limitare le operazioni di voto alle sole sedi degli Uffici consolari, come del resto disposto dalla norma. È di tutta evidenza, però, che in circoscrizioni aventi un numero elevato di elettori gli Uffici consolari andranno incontro a difficoltà di gestione dell’afflusso presso un solo seggio: per tali ragioni il Decreto non limita in principio il numero di seggi, sottoponendo però la creazione di seggi ulteriori rispetto a quello istituito presso l’Ufficio consolare ad una preventiva autorizzazione ministeriale. Una soluzione, questa, equilibrata in quanto consentirà, in caso di maggiori fondi, di trovare una soluzione al problema allestendo altri seggi. In alternativa, la bozza di Regolamento in esame permette al capo dell’Ufficio consolare di richiedere apposita autorizzazione ministeriale per estendere le operazioni di voto al seggio oltre i due giorni previsti in linea di principio.

Tenuto conto delle anticipazioni sul contenuto del Regolamento, si potrebbe configurare uno schema di voto finale sul già citato modello estone.

Il modello estone di *iVoting* ricalca il modello italiano della doppia busta cartacea, utilizzato per il

¹⁵ Gli uffici consolari possono essere di I e di II categoria. Agli uffici consolari di I categoria è preposto, quale titolare, un funzionario di carriera. Agli uffici consolari di II categoria, a contrario, un funzionario onorario. Gli uffici consolari si suddividono in Consolati generali, Consolati, Vice Consolati e Agenzie consolari (ogni ufficio superiore, nell’ordine, ha la competenza a sovrintendere su quello inferiore, cioè il Consolato Generale sovrintende Consolati, Vice Consolati e Agenzie, i Consolati sovrintendono i Vice Consolati e le Agenzie, e via dicendo). L’ufficio consolare esercita le funzioni di stato civile, notariato, amministrative e giurisdizionali.

¹⁶ Il progetto RIPA ha origine nel 2003, con l’obiettivo di migliorare l’erogazione dei servizi informatici a livello internazionale, in modo da stimolare lo sviluppo di applicazioni rivolte alle nostre comunità ed aziende internazionali (nello specifico, interessa circa 400 sedi, presenti in 120 Paesi del mondo, di: Ministero degli esteri, Ministero della Difesa, Enit, Agenzia delle Dogane). La Rete oggi fornisce a livello internazionale servizi di connettività IP e di interoperabilità di base e consente alle sedi estere la partecipazione ad applicazioni cooperative.

voto degli italiani residenti all'estero:

- il votante si collega al sito *ad hoc* e si identifica telematicamente;
- il votante vota ed il voto viene crittografato con la chiave pubblica del sistema che firma digitalmente il risultato;
- le “buste esterne” (cui è stata associata un'identità a seguito di firma digitale) sono separate dalle “buste interne” (voti crittati);
- le liste dei votanti sono compilate con le buste esterne mentre le buste interne, alle quali non è più associata l'identità del votante, sono inviate alla applicazione centrale di conteggio dei voti che possiede la chiave privata del sistema per decrittare i voti.

Al momento, però, il modello estone non sembra essere stato del tutto preso in considerazione nella bozza di Regolamento: in quest'ultimo, infatti, in base alle informazioni ad oggi a disposizione, non vi è traccia di “firma digitale”, strumento essenziale per il cittadino estone e, più in generale, per assicurare una perfetta aderenza del voto all'elettore. Il PIN per l'accesso al voto da remoto non è tecnica sufficiente e sicura. Occorre ovviamente attendere il testo finale del Regolamento.

Aspetto essenziale dell'intero sistema di voto è la predisposizione di adeguate misure a salvaguardia del dato personale trattato. Il comma 1, art. 1, del DL n. 67/2012 non fa riferimento alla necessità del coinvolgimento del Garante per la protezione dei dati personali nel processo di stesura del Regolamento attuativo della norma. Ovviamente il Garante non può essere escluso, data la delicatezza della materia e considerato il suo coinvolgimento già in ordine alla bozza di DPR recante il regolamento di attuazione della Legge n. 459/2001, che introduceva il voto per corrispondenza (Parere del Garante per la protezione dei dati personali, 17 settembre 2002, “Atti, elenchi, registri e documenti pubblici - In dirittura d'arrivo l'introduzione del voto per corrispondenza per i cittadini italiani all'estero”)¹⁷.

Lo schema di *iVoting*, contenuto nella bozza di Regolamento, però, non supera una problematica di fondo: il rispetto del principio costituzionale di segretezza del voto. Infatti, non è mai possibile tutelare pienamente la segretezza se viene consentito al cittadino di votare al di fuori dei seggi presidiati. L'*iVoting* rispetta il principio solo se, come parte della bozza di Regolamento afferma, il cittadino viene messo nelle condizioni di votare presso eventuali luoghi presidiati (ad esempio, consolati o altri luoghi specificatamente indicati dalla normativa). Soluzioni diverse non farebbero che riproporre le molte problematiche sorte negli ultimi anni a causa del voto per corrispondenza, problematiche che hanno condotto, peraltro, all'odierna riforma delle procedure elettive di COMITES e CGIE. Tali ragioni, e valutate tutte le problematiche in diritto e informatica, portano chi scrive ad esprimere: un parere positivo sulla bozza di Regolamento nelle parti in cui configura modalità di *iVoting* in seggi presidiati; negativo nei restanti casi di utilizzo dello strumento *iVoting*. Obiezione a tale posizione può derivare da chi sostiene che il voto degli italiani all'estero detiene caratteri peculiari connessi il più delle volte alle enormi distanze che separano i nostri connazionali dai consolati o ambasciate nelle quali, eventualmente, porre in essere seggi presidiati. L'*iVoting* da remoto, pertanto, annullerebbe il problema della distanza e, quindi, del recarsi fisicamente ad un seggio molto lontano. Ma ragionare solo sulle distanze chilometriche e non in ordine al, ben più rilevante, problema della segretezza e certezza del voto appare pretestuoso. Detto in altre parole,

¹⁷ Il Parere è visionabile all'URL: <http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1066114>, consultato nel mese di aprile 2013.

ai problemi di non segretezza e incertezza del voto emersi negli anni a seguito dell'introduzione del voto per corrispondenza sostituiremmo quelli, della medesima natura, che scaturirebbero con l'*iVoting* ammesso in seggi non presidiati. Cambia la "tecnologia del problema" (dalla carta del plico postale al *bit* trasmesso in Rete), ma i problemi operativi e di contrasto con i principi costituzionali rimangono intatti.

È quindi auspicabile che il Regolamento, adeguatamente modificato in base all'odierna bozza, ammetta solo modalità *iVoting* in seggi presidiati o, anche, modalità *eVoting* in seggi presidiati con urne aventi caratteristiche funzionali simili a quella messicana, già descritta.

Occorre ora soffermarsi sull'applicabilità del CAD alle elezioni dei COMITES e CGIE.

L'art. 2, comma 6, del CAD dispone la sua inapplicabilità in materia di "consultazioni elettorali". Data la (voluta) genericità della locuzione adottata dal legislatore ("consultazioni elettorali") occorre ritenere inapplicabile il CAD anche nel caso delle elezioni dei componenti di COMITES e CGIE. La norma, però, non ha una portata "assoluta", considerata la complessità del sistema digitale pubblico nel quale una molteplicità di strumenti ICT intervengono costantemente e congiuntamente in ogni attività. Il CAD, pertanto, produce effetti, con diversi gradi di consapevolezza del Legislatore, anche in caso di "consultazioni elettorali" per i COMITES e CGIE, sotto molteplici profili. Il voto elettronico per le elezioni di COMITES e CGIE, come emerge dalla bozza di Regolamento, di certo è in linea con:

- il contenuto dell'art. 9 CAD, in tema di partecipazione democratica elettronica, secondo il quale le Pubbliche Amministrazioni devono favorire 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;
- il contenuto dell'art. 12 CAD, in tema di organizzazione delle Amministrazioni, in base al quale quest'ultime 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, nel rispetto dei principi di uguaglianza e di non discriminazione, nonché per la garanzia dei diritti dei cittadini e delle imprese sanciti dal CAD;
- il contenuto dell'art. 15 CAD, in tema di riorganizzazione strutturale e gestionale delle Pubbliche Amministrazioni che deve essere volta al perseguimento degli obiettivi di cui al citato art. 12, e avvenire 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 processo di digitalizzazione;
- il contenuto dell'art. 63 CAD, in tema di servizi pubblici in Rete, in base al quale le Pubbliche Amministrazioni centrali individuano le modalità di erogazione dei servizi in Rete in base a criteri di valutazione di efficacia, economicità ed utilità e nel rispetto dei principi di eguaglianza e non discriminazione, tenendo comunque presenti le dimensioni dell'utenza, la frequenza dell'uso e l'eventuale destinazione all'utilizzazione da parte di categorie in situazioni di disagio¹⁸.

¹⁸ Riassumendo, la norma distingue tre elementi caratteristici del servizio in Rete, che la bozza di Regolamento appare rispettare: "Il primo elemento è dato dal fatto che, da un punto di vista soggettivo, i servizi in Rete sono erogati dalle Pubbliche Amministrazioni centrali. Il secondo elemento si deduce dalla considerazione secondo cui, da un

-
- il contenuto degli artt. 74 e 85 CAD, in tema di RIPA, poiché viene sfruttata al meglio quest'ultima e i suoi caratteri di infrastruttura di connettività (quindi interconnessa al SPC¹⁹), che collega le Pubbliche Amministrazioni con gli uffici italiani all'estero, garantendo adeguati livelli di sicurezza e qualità.
 - il contenuto dell'art. 49 CAD, in tema di segretezza nelle trasmissioni telematiche, in base al quale gli addetti alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono prendere cognizione della corrispondenza telematica, duplicare con qualsiasi mezzo o cedere a terzi a qualsiasi titolo informazioni anche in forma sintetica o per, estratto sull'esistenza o sul contenuto di corrispondenza, comunicazioni o messaggi trasmessi per via telematica, salvo che si tratti di informazioni per loro natura o per espressa indicazione del mittente destinate ad essere rese pubbliche;
 - il contenuto dell'art. 60 CAD, in tema di basi di dati di interesse nazionale, definibili come l'insieme delle informazioni raccolte e gestite digitalmente dalle Pubbliche Amministrazioni, omogenee per tipologia e contenuto e la cui conoscenza è utilizzabile dalle Pubbliche Amministrazioni, anche per fini statistici, per l'esercizio delle proprie funzioni e nel rispetto delle competenze e delle normative vigenti. Ferme le competenze di ciascuna Pubblica Amministrazione, le basi di dati di interesse nazionale costituiscono, per ciascuna tipologia di dati, un sistema informativo unitario che tiene conto dei diversi livelli istituzionali e territoriali e che garantisce l'allineamento delle informazioni e l'accesso alle medesime da parte delle Pubbliche Amministrazioni interessate. La realizzazione di tali sistemi informativi e le modalità di aggiornamento sono attuate secondo le regole tecniche sul Sistema Pubblico di Connettività (SPC)²⁰ e secondo le vigenti regole del Sistema statistico nazionale;
 - il contenuto dell'art. 64 CAD, in tema di strumenti di identificazione del cittadino nei servizi in Rete (come quello di *iVoting*), identificazione possibile non solo tramite Carta di Identità Elettronica (CIE) e Carta Nazionale dei Servizi (CNS) ma anche con strumenti diversi, purché

punto di vista strutturale, i servizi in Rete sono attività di trasmissione ed elaborazione di informazioni. Il terzo elemento, infine, definisce che, da un punto di vista oggettivo, con riferimento all'attività amministrativa, sono servizi pubblici in Rete le attività giuridiche dell'Amministrazione alla cui erogazione corrisponde un diritto soggettivo del beneficiario" (G. CANGELOSI, *I servizi pubblici sanitari: prospettive e problematiche della telemedicina*, in "Il Diritto di famiglia e delle persone", 1, 2007, p. 439).

¹⁹ Il Sistema Pubblico di Connettività (SPC) ha visto la luce in Italia nel 2007 ed in base all'art. 73 del 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". L'SPC ha sostituito la Rete Unitaria per la Pubblica Amministrazione (RUPA), operativa in Italia dal marzo del 2000, ovvero 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 (Cfr. C. RABBITO, *L'informatica al servizio della pubblica amministrazione e del cittadino*, Bologna, Gedit Edizioni, 2007; G. RIEM, *Sistema Pubblico di Connettività*, in R. BORRUSO, G. RIEM, A. SIROTTI GAUDENZI, P. VICENZOTTO (a cura di), *Glossario di diritto delle nuove tecnologie e dell'eGovernment*, Milano, Giuffrè Editore, 2007, pp. 460-463).

²⁰ L'art. 60 CAD individua come base di dati di interesse nazionale l'Anagrafe nazionale della popolazione residente, base di dati che ovviamente detiene un ruolo essenziale nei processi di voto anche per gli italiani all'estero. Eventuali problematiche di iscrizione all'AIRE o all'Anagrafe nazionale potranno essere risolte solo se le due anagrafi potranno dialogare, quindi se saranno costruite secondo parametri di interoperabilità.

-
- tali strumenti consentano l'individuazione del soggetto che richiede il servizio;
- il contenuto dell'art. 62 CAD, in tema di Anagrafe nazionale della popolazione residente (ANPR) istituita con DPCM 23 agosto 2013, n.109, (entra in vigore il 16 ottobre 2013)²¹ e che subentra, entro il 31 dicembre 2014, anche all'AIRE e alle anagrafi della popolazione residente e dei cittadini italiani residenti all'estero tenute dai comuni. Ulteriori DPCM definiranno meglio le garanzie e le misure di sicurezza da adottare nel trattamento dei dati personali, le modalità e i tempi di conservazione dei dati e l'accesso agli stessi da parte delle Pubbliche Amministrazioni per le proprie finalità istituzionali. Appare chiaro come il CAD risulti comunque coinvolto nell'attuazione del processo di innovazione tecnologica del voto per i COMITES e CGIE. Allontanarsi dalle disposizioni citate, in caso di *eVoting*, a parere di chi scrive non appare una strada percorribile dal Legislatore.

Occorre ora soffermarsi sulla (non meditata) tempistica della riforma *eVoting* dettata dal legislatore con il comma 1, art. 1, del DL n. 67/2012.

Abbiamo già evidenziato come le elezioni dei COMITES e CGIE dovranno avvenire entro il 2014. Pertanto, è lecito supporre che il Regolamento attuativo dovrà essere emanato entro l'anno 2013, diversamente diventerà particolarmente complesso, e rischioso informaticamente, predisporre piattaforme di voto elettronico non adeguatamente testate. L'unica alternativa diventerà il possibile rinvio delle elezioni, pratica non inusuale nel settore, con chiara lesione del diritto alla rappresentanza nei COMITES e CGIE di cui sono titolari gli italiani residenti all'estero.

Tralasciando ora la problematica regolamentare, nelle sue varie sfaccettature, appare comunque chiaro come in Italia, ad oggi, la normativa in tema di voto dei residenti all'estero (quantomeno sotto il profilo dell'elezione di COMITES e CGIE) sia assolutamente aperta a innovazioni procedurali, anche in tema di voto, in grado di garantire maggiore efficienza, efficacia, economicità, imparzialità, trasparenza, semplificazione dell'*agere* amministrativo e partecipazione democratica dei cittadini, anche con l'ausilio e supporto di privati, come possono essere le aziende fornitrici dei macchinari di *iVoting/eVoting* e i gestori dei servizi RIPA.

A parere di chi scrive, dunque, la strada normativa è aperta anche in Italia per una piena e legale affermazione di sistemi di votazione elettronica, sia per i cittadini all'estero che per quelli residenti e votanti nel territorio nazionale. Diversamente opinando si lederebbe il principio di uguaglianza (art. 3 Cost.) nel caso in cui si permettesse ai soli italiani all'estero di esercitare il loro diritto di voto con modalità semplificate e, sotto notevoli profili, più sicure (cioè quelle informatiche e telematiche) rispetto agli italiani residenti sul territorio nazionale. In futuro, peraltro, decidere di non utilizzare in Italia, per qualsivoglia tornata elettorale o *referendum*, gli strumenti *eVoting* testati per i COMITES e CGIE significherebbe ledere palesemente anche il principio costituzionale di buon andamento (art. 97 Cost.) cui ogni Pubblica Amministrazione deve rifarsi: investire milioni di euro per innovare le modalità di voto solo per elezioni sporadiche, come quelle di COMITES e CGIE significa, infatti, non utilizzare al meglio le risorse pubbliche. Alla luce di tali considerazioni

²¹ L'allegato al DPCM n. 109/2013 descrive le fasi di attuazione dell'ANPR, nonché i sistemi di sicurezza iniziali e le fasi progettuali con cui sarà istituita l'Anagrafe. Tutte le funzioni connesse alla gestione, all'aggiornamento e alla consultazione dell'ANPR sono affidate al CNSD (Centro Nazionale Servizi Demografici), costituito con decreto del Ministro dell'Interno del 23 aprile 2002 presso la Direzione Centrale per i Servizi Demografici. Al DPCM ha fatto seguito la Circolare informativa n. 19/2013 del 3 ottobre 2013 del Ministero degli Interni - Dipartimento per gli affari esterni e territoriali.

potrebbero anche aprirsi spiragli di incostituzionalità di norme adottate in futuro dal Legislatore in materia di voto per i residenti in Italia, nel caso in cui non obblighino all'uso delle piattaforme informatiche e telematiche eventualmente già esistenti.

3. Futuro e prospettive dell'eVoting

Nel mondo i vari Paesi stanno procedendo a velocità diverse in tema di voto elettronico.

Vi sono Paesi nei quali esso costituisce una piena realtà, non solo sul piano tecnologico ma anche sul piano normativo e del valore legale attribuito a tali sistemi innovativi. Generalmente si tratta di “Paesi emergenti”, come Brasile o Messico. La ragione di tale fenomeno la si comprende facilmente: in questi Stati, come in altri latinoamericani, “l'implementazione del voto elettronico è gestita dagli organismi elettorali, permanenti, altamente specializzati e dedicati esclusivamente alla gestione elettorale, una situazione che non si riscontra in nessuno dei Paesi europei”²². Rimanendo negli esempi fatti, in Brasile infatti abbiamo il Tribunale Elettorale Superiore e i Tribunali Elettorali Regionali, in Messico gli IEPC statali.

Vi sono, poi, altri Paesi nei quali la sperimentazione vi è stata e in taluni casi si è giunti ad una piena affermazione sociale e giuridica del voto elettronico, per poi, però, arrestarsi o fare un totale *revirement*. In tale categoria di certo rientrano molti Paesi europei, ancora radicati alla tradizione cartacea, restii al cambiamento, non solo tecnologico e organizzativo ma, soprattutto, culturale, come l'Italia o, tra gli esempi di un ritorno al passato in tema di voto elettronico, l'Olanda e l'Irlanda.

Vi sono, infine, tutti i restanti Paesi nei quali il dibattito e la sperimentazione del settore del voto elettronico non accennano ad avviarsi.

I Paesi più sviluppati, però, non possono non restare al passo di quelli emergenti. Devono, se in ritardo, rimettersi in pari. È il caso dell'Italia.

I tempi per l'avvento nel nostro Paese di una compiuta legislazione in tema di voto elettronico, da considerarsi tale ultima locuzione nella sua accezione più completa, ovvero quella contenuta nelle Linee Guida del Consiglio d'Europa del 2004 (“un'elezione o un *referendum* in modalità elettronica che prevede l'utilizzo di mezzi elettronici almeno al momento della registrazione del voto nell'urna”), appaiono maturi. Il riconoscimento del valore legale al voto elettronico e il suo potere sostitutivo del voto cartaceo possono, dunque, divenire realtà in Italia, in quanto sussistono quattro elementi che rendono oramai improcrastinabile una disciplina di settore:

- 1) l'esistenza di una cogente normativa nel CAD, già citata, volta a incentivare la “partecipazione democratica elettronica” dei cittadini (art. 9) e le attività di reingegnerizzazione e informatizzazione delle attività e dei servizi al cittadino, ivi compresi i processi elettorali (art. 12, comma 1, CAD);
- 2) se a seguito della riforma costituzionale del 2001 le Regioni a Statuto speciale, come il Trentino Alto Adige e il Friuli Venezia-Giulia, hanno visto attribuita l'autonomia di scelta delle moda-

²² F. BARRIENTOS DEL MONTE, *El “no al voto electrónico”: ¿por qué en algunos países la implementación del voto electrónico es exitosa y en otros fracasa?*, in AA.VV., *Tecnología y participación ciudadana en la construcción democrática*, Guadalajara (Mexico), IECP Jalisco e PNUD México, 2011, pp. 97-115 (traduzione nostra).

-
- lità di voto, sarebbe quantomeno discutibile non permettere ai restanti cittadini italiani ed alle restanti istituzioni ed enti pubblici di poter optare nella scelta tra il sistema di voto tradizionale e quello innovativo elettronico, ovviamente con pieno valore legale, il tutto da disciplinare con legge *ad hoc*: principi come quelli di buon andamento della Pubblica Amministrazione (art. 97 Cost.) o quelli di efficacia, efficienza ed economicità amministrativa di cui alla Legge n. 241/1990 devono costituire presupposto di una diffusione nazionale di strumenti atti a realizzarli, come nel caso del voto elettronico;
- 3) come visto, la normativa in tema di elezioni degli italiani all'estero permette già l'*eVoting*, appare discriminatorio che il diritto di votare elettronicamente non venga riconosciuto anche agli italiani residenti sul territorio nazionale; il diritto di voto degli italiani all'estero ha vissuto un inizio secolo di continue e profonde innovazioni, alle quali non ha fatto eco un'eguale innovazione nel voto per i residenti in Italia, configurando una sorta di paradosso: oggi appare sempre più tutelato e al passo con i tempi il diritto di voto degli italiani all'estero rispetto a chi vive sul territorio nazionale;
 - 4) da un punto di vista tecnologico, sussistono nel mondo strumentazioni elettroniche già in linea con i requisiti giuridici di cui all'art. 48 Cost. e con i principi in tema di *eVoting* espressi dal Consiglio d'Europa nel 2004: *in primis*, si consideri l'urna elettronica messicana, sperimentata nella sua ultima versione nel mese di luglio 2012 nel Paese centro-americano e nel maggio 2013 nei Comuni salentini di Martignano e Melpignano.

Al di là delle questioni informatiche e giuridiche sottese all'introduzione di qualsiasi forma di sperimentazione di *eVoting*, il vero problema è rappresentato dalla fiducia degli elettori, senza la quale anche le piccole problematiche possono essere enfatizzate e condurre all'arresto di ogni processo innovativo. In Italia nulla è stato fatto negli ultimi anni in questa direzione. Il dibattito non solo si è arrestato da tempo, ma non vi sono neanche slanci in tale direzione. Occorre ripartire con una riflessione comune sui benefici dell'*eVoting*. Caso emblematico l'odierna introduzione dell'*eVoting* per le elezioni dei COMITES e CGIE, una rilevante novità nel nostro ordinamento che sta passando del tutto inosservata agli occhi della Nazione, con ogni discussione relegata solo agli "addetti ai lavori" (tecnici, politici, giuristi).

Occorre ripetere e ripeterci che è arrivato il momento di riavviare "un dibattito serio per semplificare e rendere più efficienti le procedure elettorali utilizzando gli ausili che la tecnologia offre, senza prefigurare a priori scenari catastrofici o soluzioni semplicistiche, ma tenendo in considerazione, attraverso un'analisi costi-opportunità, le prospettive offerte dalle procedure di voto informatizzate"²³.

Rimanere ancora sordi alle istanze, forse meglio dire "necessità", di cambiamento vorrà dire non porre le basi per una reale costruzione di una "cittadinanza digitale" o, meglio, una reale "cittadinanza digitale europea", uno degli elementi che maggiormente caratterizzerà il cittadino degli "Stati Uniti d'Europa"²⁴. Vorrà anche dire condurre l'Italia ad un ulteriore arretramento in termini

²³ A. SARAI, *Democrazia e tecnologie. Il voto elettronico*, cit., p. 110.

²⁴ Cfr. E. FAZI, G. PITTELLA, *Breve storia del futuro degli Stati Uniti d'Europa*, Roma, Fazi Editore, 2013. Il lavoro intende raccontare, con spirito divulgativo e al contempo critico, le svolte inaspettate che hanno interessato l'Europa nel 2012, mutando considerevolmente lo scenario mondiale nel prossimo futuro. Gli Autori aprono dunque il dibattito in ordine alla *road-map*, preparata dal Presidente del Consiglio Europeo assieme a quelli della Commissione Europea,

di civiltà, tutela dei diritti e risparmio del denaro pubblico rispetto ai restanti Stati sviluppati e, sotto i diversi aspetti di cui abbiamo trattato, rispetto a molti Stati in via di sviluppo.

Bibliografia

- AINIS M., *La legalità ferita. Relazione introduttiva all'“Assemblea dei 1000”*, Roma, 17 Giugno 2005, disponibile all'URL: <http://archivio.rivistaic.it/dibattiti/attualita/ainis.html>, consultato nel mese di marzo 2013.
- ALEMANNO G.S., *Il Codice dell'amministrazione digitale*, Pescara-Bergamo, CEL, 2011.
- ALVAREZ R.M., HALL T.E., *Point, Click, and Vote. The Future of Internet Voting*, Washington DC (USA), Brookings Institution, 2004.
- ALVAREZ R.M., HALL T.E., TRECHSEL A.H., *Internet Voting in Comparative Perspective: The Case of Estonia*, in “Political Science & politics”, 3, 2009, pp. 497-505.
- AMATO MANGIAMELI A.C., *Informatica giuridica*, Torino, Giappichelli Editore, 2010.
- BARRAT I ESTEVE J., GOLDSMITH B., TURNER J., *International Experience with E-Voting: Norwegian E-Vote Project*, Washington DC (USA), IFES, 2012, disponibile all'URL: http://www.ifes.org/Content/Publications/News-in-Brief/2012/June/~media/Files/Publications/Reports/2012/EVote_International_Experience_2012.pdf, consultato nel mese di aprile 2013.
- BARRIENTOS DEL MONTE F., *El “no al voto electrónico”: ¿por qué en algunos países la implementación del voto electrónico es exitosa y en otros fracasa?*, in AA.VV., *Tecnología y participación ciudadana en la construcción democrática*, Guadalajara (Mexico), IECP Jalisco e PNUD México, 2011, pp. 97-115.
- BETTINELLI E., *La lunga marcia del voto elettronico in Italia*, in “Quaderni dell'osservatorio elettorale”, 46, 2002, pp. 5-48.
- ID., *Il sistema e-poll nello spazio elettorale europeo: dalla prospettiva al progetto*, in “Il politico”, 1, 2003, pp. 39-63.
- BICKNER C., *Down By Law*, in “A List Apart Magazine”, 104, 2001, disponibile all'URL: <http://www.alistapart.com/articles/downbylaw/>, consultato nel mese di agosto 2012.
- BOBBIO N., *Teoria generale della politica*, Torino, Einaudi, 1999.
- BRAUN N., BRANDLI D., *Swiss E-Voting Pilot Projects: Evaluation, Situation Analysis and How to Proceed*, in KRIMMER R. (a cura di), *Electronic Voting 2006*, Bonn, Gesellschaft fur Informatik, 2006, pp. 27-36.
- BRAUN N., *E-Voting: Switzerland's Projects and Their Legal Framework*, in PROSSER A., KRIMMER R., *Electronic Voting in Europe: Technology, Law, Politics and Society*, Bonn, Gesellschaft fur Informatik, 2004, pp. 43-52.
- BRUNET F., ARNOUX V., *Management et droit dans la net économie*, Paris, Economica, 2002.
- BUCCARELLA M.M., *E-Poll: una soluzione elettronica per la democrazia*, in “Diritto & Diritti”, novembre 2002, disponibile all'URL: <http://www.diritto.it/materiali/tecnologie/buccarella5.html>, consultato nel mese di marzo 2013.
- ID., *Il voto elettronico: una soluzione per la democrazia*, in “Diritto & Diritti”, luglio 2012, disponibile all'URL: <http://www.diritto.it/materiali/tecnologie/buccarella4.html>, consultato nel mese di aprile 2013.
- BUCHSTEIN H., *Modernisierung Der Demokratie Durch E-Voting?*, in “Leviathan: Zeitschrift fur Sozialwissenschaft”, 4, 2001, pp. 147-155.
- CANGELOSI G., *I servizi pubblici sanitari: prospettive e problematiche della telemedicina*, in “Il Diritto di famiglia e delle persone”, 1, 2007, pp. 431-481.
- CIAURRO G.F., *Prospettive di ammodernamento dei procedimenti elettorali*, in AGOSTA A., LANCHESTER F., SPREAFICO F. (a cura di), *Elezioni e automazione. Tutela della regolarità del voto e prospettive di innovazione tecnologica*, Milano, Franco Angeli, 1989, pp. 68-80.
- COGO G., *La cittadinanza digitale. Nuove opportunità tra diritti e doveri*, Roma, Edizioni della Sera, 2010.

della Banca Centrale Europea e dell'Eurogruppo, per giungere all'unità politica dell'Europa sulla linea di quanto suggerito nel Rapporto della Commissione “*A Blueprint for a deep and genuine EMU: Launching a European debate*” (Comunicazione della Commissione, COM(2012) 777 final, del 28 novembre 2012).

-
- COSTANZO P., *La democrazia elettronica (note minime sulla cd. E-democracy)*, in “Il diritto dell’informazione e dell’informatica”, 3, 2003, pp. 465-486.
 - CUOCOLO L., *Voto elettronico e postdemocrazia nel diritto costituzionale comparato*, in “Diritto pubblico comparato ed europeo”, 1, 2008.
 - DAHLBERG L., SIAPERA E., *Radical Democracy and the Internet: Interrogating Theory and Practice*, New York, Palgrave Macmillan, 2007.
 - DAMONTE A., *Il Rapporto Sulle Regioni*, Roma, Formez, 2002, disponibile all’URL: [http://db.formez.it/storicofontinor.nsf/8804ac899ac04f07c12569f40030aaca/D0604C6B1B27971AC1256C5A002E36D1/\\$file/Rapporto%20Regioni.pdf](http://db.formez.it/storicofontinor.nsf/8804ac899ac04f07c12569f40030aaca/D0604C6B1B27971AC1256C5A002E36D1/$file/Rapporto%20Regioni.pdf), consultato nel mese di agosto 2012.
 - DE PIETRO L. (a cura di), *Dieci lezioni per capire e attuare l’eGovernment*, Venezia, Marsilio, 2011.
 - DI MARIA E., MICELLI S. (a cura di), *Le frontiere dell’eGovernment: cittadinanza elettronica e riorganizzazione dei servizi in rete*, Milano, Franco Angeli, 2004.
 - DUNI G., *La teleamministrazione come terza fase dell’informatica amministrativa. Dalla “informazione automatica” sulle procedure burocratiche al procedimento in forma elettronica*, in ID. (a cura di), *Dall’informatica amministrativa alla teleamministrazione*, Roma, IPZS - Libreria dello Stato, 1992, pp. 15-24.
 - ENGUEHARD C., *Le vote électronique en France: opaque & invérifiable*, 8 dicembre 2006, disponibile all’URL: <http://pageperso.lina.univ-nantes.fr/info/perso/permanents/enguehard>, consultato nel mese di agosto 2012.
 - ID., *Introduction à l’analyse de chimères technologiques, le cas du vote électronique*, in “Cahiers Droit, Sciences & Technologies”, 3, 2010, pp. 261-278.
 - ID., *Trasparenza, elezioni e voto elettronico*, in FOREY E., GESLOT C., (a cura di), *Internet, machines à voter et démocratie*, Paris, L’Harmattan, pp. 85-108.
 - FAIRWEATHER B., ROGERSON S., *Internet Voting. Well at Least It’s Modern*, in “Representation”, 3, 2009, pp. 182-195.
 - FALCÃO J., FARIA J.P., LEITÃO M.J., PIMENTA A., CARRAVILLA M.A., *Auditing E-Voting Pilot Processes and Systems at the Elections for the European Parliament and for the Portuguese Parliament* in RENU J.M. (a cura di), *E-Voting: The Last Electoral Revolution*, Barcelona, ICPS, 2008, disponibile all’URL: http://www.academia.edu/2821776/Auditing_e-Voting_Pilot_Processes_and_Systems_at_the_Elections_for_the_European_Parliament_and_for_the_Portuguese_Parliament, consultato nel mese di aprile 2013.
 - FAZI E., PITTELLA G., *Breve storia del futuro degli Stati Uniti d’Europa*, Roma, Fazi Editore, 2013.
 - FERNÁNDEZ RODRÍGUEZ J.J., BARRAT I ESTEVE J., FERNÁNDEZ RIVEIRA R.M., RENU I VILLAMALA J.M., *Voto Electrónico. Estudio Comparado En Una Aproximación Jurídico-Política (Desafíos Y Posibilidades)*, Santiago de Querétaro (Mexico), Fundación Universitaria de Derecho, Administración y Política, 2007.
 - FIGUEROA PADILLA J.T., *Democracia digital: el uso de un sistema electrónico para la recepción del voto en Jalisco*, in AA.VV., *Tecnología y participación ciudadana en la construcción democrática*, cit., pp. 133-139.
 - FINOCCHIARO G., *La metafora e il diritto nella normativa sulla cosiddetta “firma grafometrica”*, in “Il diritto dell’informatica e dell’informazione”, 1, 2013, pp. 1-16.
 - FROSINI V., *La democrazia del XXI secolo*, Roma, Edizioni Ideazione, 1997.
 - ID., *La democrazia informatica non è autoritaria, ma di massa*, in “Telèma”, 14, 1998, pp. 101-104.
 - FROSINI T.E., *La libertà informatica: brevi note sull’attualità di una teoria giuridica*, in “Informatica e Diritto”, 1/2, 2008, pp. 87-97.
 - FURLANI S., *L’adozione di macchinari per l’espressione del voto in altri contesti nazionali: l’esperienza delle elezioni per il Bundestag*, in A. AGOSTA, LANCHESTER F., SPREAFICO F. (a cura di), *Elezioni e automazione. Tutela della regolarità del voto e prospettive di innovazione tecnologica*, cit., pp. 118-124.
 - GELPI A., *Elezioni, censimenti, referendum*, in “Stat. Civ. It.”, 1972, pp. 110-111.
 - GONGGRIJP R., HENGEVELD W.J., *Nedap/Groenendaal Es3b Voting Computer*, 2007, in http://wijvertrouwenstemcomputersniet.nl/images/c/ce/ES3B_EVT07.pdf, consultato nel mese di agosto 2012.
 - GRASSI ORSINI F., NICOLOSI G., *Luci ed ombre della cyber politica: i governi online. Il partito telematico*, 2002, disponibile all’URL: <http://www.storiaefuturo.com/arretrati/2002/01/01/006/0003.html>, consultato nel mese di agosto 2012.
 - GRATTELLI A., *Il valore del voto: nuove tecnologie e partecipazione elettorale*, Padova, Cedam, 2005.
 - GROSSMAN L.K., *The Electronic Republic. Reshaping Democracy in the information Age*, New York, Penguin Group USA, 1996.

-
- GUTIÉRREZ P., *Perspectivas sobre el uso de la tecnología móvil e internet en procesos electorales en el contexto de las misiones de observación de la OEA*, in AA.VV., *Tecnología y participación ciudadana en la construcción democrática*, cit., pp. 61-75.
 - HINNA L., LASALVIA M., *La riforma della pubblica amministrazione tra diritto e management: la riforma Brunetta aggiornata con le ultime norme sul lavoro pubblico (Legge 183/2010), la class action (D. lgs. 198/2009), il Codice dell'amministrazione digitale (D. lgs. 235/2010) e la Carta dei doveri delle amministrazioni pubbliche*, Roma, EPC, 2011.
 - HOF S., *E-Voting and Biometric Systems?*, in PROSSER A., KRIMMER R. (a cura di), *Electronic Voting in Europe: Technology, Law, Politics and Society*, cit., pp. 63-72.
 - JONAS H., *Das Prinzip Verantwortung*, Frankfurt am Main, Insel Verlag, 1979, trad. it., *Il principio responsabilità. Un'etica per la civiltà tecnologica*, Torino, Einaudi, 1990.
 - KENSKI K., *To I-Vote or Not to I-Vote? Opinions About Internet Voting from Arizona Voters*, in "Social Science Computer Review", 3, 2005, pp. 293-303.
 - KRIMMER R., TRIESSNIG S., VOLKAMER M., *The development of remote eVoting around the world: a review of roads and directions*, in ALKASSAR A., er VOLKAM M. (a cura di), *eVoting and Identity*, Berlin, Springer-Verlag, 2007, pp. 1-15.
 - KUMAR S., WALIA E., *Analysis of Electronic Voting System in Various Countries*, in "International Journal on Computer Science and Engineering", 5, 2011, pp. 1825-1830.
 - LADYGIN L., *The Russian Electronic Voting System*, 1 agosto 2012, disponibile all'URL: <http://www.e-voting.cc/en/the-russian-electronic-voting-system/>, consultato nel mese di agosto 2012.
 - LIMONE D.A., *Rivoluzioni organizzative: la teoria dei paradigmi di Thomas Kuhn*, in "eGov – Cultura e tecnologie per l'innovazione", 1/2, 2008, pp. 17-19.
 - LUHMANN N., *I Diritti fondamentali come istituzione*, trad. it., Bari, Edizioni Dedalo, 2002.
 - MACRÌ I., MACRÌ U., PONTEVOLPE G. (a cura di), *Il nuovo codice dell'amministrazione digitale: le tecnologie informatiche e le norme che ne disciplinano l'uso*, Assago, IPSOA, 2011.
 - MARONGIU D., *Gli atti amministrativi ad elaborazione elettronica: la compilazione del "pre-software" in lingua italiana*, marzo 2008, disponibile all'URL: <http://www.cesda.it/quadernidae/>, consultato nel mese di aprile 2013.
 - MARTIN VARGAS M.A., DE ALMEIDA ANHAIA A., *Brasil y el voto digital*, in AA.VV., *Tecnología y participación ciudadana en la construcción democrática*, cit., pp.117-132.
 - MARVIN C., SIMONSON P., *Voting Alone: The Decline of Bodily Mass Communication and Public Sensationalism in Presidential Elections*, in "Communication and Critical/Cultural Studies", 1, 2004, pp. 127-150.
 - MASTROLONARDO R., *Ma non chiamatelo voto elettronico*, in "Monthly vision", marzo 2006, pp. 45-48.
 - MCCARTHY J., *Electronic Voting in Ireland. Summary of Costs*, 2004, disponibile all'URL: <http://www.evoting.cs.may.ie/Documents/CostofElectronicvotingAsOfMay.pdf>, consultato nel mese di agosto 2012.
 - OOSTVEEN A.M., VAN DEN BESSELAAR P., *Internet Voting Technologies and Civic Participation: The Users' Perspective*, in "Javnost", 1, 2004, pp. 61-78.
 - OROFINO A.G., *Il voto elettronico*, in CASSANO G. (a cura di), *Il diritto delle nuove tecnologie informatiche e dell'Internet*, Milano, Ipsoa, 2002, pp. 232-247.
 - ID., *L'e-vote*, in Sarzana F. (a cura di), *E-Government. Profili teorici ed applicazioni pratiche del Governo digitale*, Piacenza, La Tribuna, 2003, pp. 361-383.
 - PALMIRANI M., *Prefazione*, in PALMIRANI M., MARTONI M. (a cura di), *Il cittadino elettronico e l'identità digitale nell'e-governance*, Bologna, Gedit edizioni, 2006, pp. 7-9.
 - PASQUINO G. (a cura di), *Strumenti della democrazia*, Bologna, Il Mulino, 2007.
 - PITTERI D., *Democrazia elettronica*, Roma-Bari, Laterza, 2007.
 - PREITE G., *Il riconoscimento biometrico. Sicurezza versus Privacy*, Trento, Editrice UNI Service, 2008.
 - PUDDU S., *Contributo ad uno studio sull'anormalità dell'atto amministrativo informatico*, Napoli, Jovene, 2006.
 - RABBITO C., *L'informatica al servizio della pubblica amministrazione e del cittadino*, Bologna, Gedit Edizioni, 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'eGovernment*, Milano, Giuffrè Editore, 2007, pp. 460-463.
 - RODOTÀ S., *La sovranità nel tempo della tecnopolitica. Democrazia elettronica e democrazia rappresentativa*, in "Politica del Diritto", 4, 1993, pp. 569-600.
 - ID., *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Roma-Bari, Laterza, 2004.
 - ID., *I sette peccati capitali di Internet (e le sue virtù)*, in "La Repubblica", 6 marzo 2007.
-

-
- ROMANO A., MARASSO L., MARINAZZO M., *Italia chiama eGovernment*, Milano, Guerini e Associati, 2008.
 - ROSSANO R., *Teledemocrazia: il voto elettronico*, in “Rass. Parl.”, 1, 1994, pp. 97-106.
 - ROZO ACUÑA E., *Habeas data costituzionale: nuova garanzia giurisdizionale del diritto pubblico latinoamericano*, in “Diritto pubblico comparato ed europeo”, 4, 2002, pp. 1829-1872.
 - RUSSI L., *Voto e scrutinio elettronico: problemi tecnici ed organizzativi*, in AGOSTA A., LANCHESTER F., SPREAFICO A. (a cura di), *Elezioni e automazione. Tutela della regolarità di voto e prospettive di innovazione tecnologica*, cit., pp. 81-104.
 - SARAI A., *Democrazia e tecnologie. Il voto elettronico*, Bologna, Esculapio, 2008.
 - SARTORI G., *Democrazia. Cosa è*, Milano, Rizzoli, 1993.
 - SCARAMOZZINO P., *Le proposte per il voto elettronico*, in “Nomos”, 1, 1988, pp. 77-82.
 - SCHEER L., *La democrazia virtuale*, trad. it., Genova, Costa & Nolan, 1997.
 - SINGH R., *Democracia electrónica en América Latina en la intersección de la democracia inclusiva y la web 2.0*, in AA.VV., *Tecnología y participación ciudadana en la construcción democrática*, cit., pp. 25-38.
 - SMITH A.D., CLARK J.S., *Revolutionising the Voting Process through Online Strategies*, in “Online Information Review”, 5, 2005, pp. 513-530.
 - SPANU M., *Il Procedimento elettorale: nodi problematici*, in AGOSTA A., LANCHESTER F., SPREAFICO A. (a cura di), *Elezioni e automazione. Tutela della regolarità di voto e prospettive di innovazione tecnologica*, cit., pp. 35-52.
 - ID., *La gestione elettronica delle operazioni di votazione e scrutinio*, in “Nuova Rassegna di legislazione, dottrina e giurisprudenza”, 3, 1986, pp. 353-357.
 - TEDESCHI M., *E-democracy*, in L. DE PIETRO (a cura di), *Dieci lezioni per capire e attuare l'eGovernment*, cit., pp. 155-170.
 - TEDESCO V., *Ancora un altro successo del voto elettronico nelle Università*, in “Diritto & Diritti”, 6 novembre 2002, disponibile all'URL: http://www.diritto.it/osservatori/voto_teleumatico/tesesco6.html, consultato nel mese di agosto 2012.
 - ID., *eGovernment e voto elettronico. Le applicazioni in Europa e nel Mondo. L'implementazione nelle Università: l'esempio dell'Università di Pisa. La programmazione delle attività e la valutazione dei risultati. Come la e-democracy sta cambiando il modo di vivere della società*, in “Diritto & Diritti”, 2002, disponibile all'URL: http://www.diritto.it/osservatori/voto_teleumatico/, consultato nel mese di agosto 2012.
 - TILLY C., *La democrazia*, trad. it., Bologna, Il Mulino, 2009.
 - TRUCCO L., *Le nuove tecnologie salveranno il voto all'estero degli italiani?*, in “Forum di Quaderni costituzionali”, 6 gennaio 2013, disponibile all'URL: http://www.forumcostituzionale.it/site/images/stories/pdf/documenti_forum/paper/0387_trucco.pdf, consultato nel mese di aprile 2013.
 - VIRILIO P., *La vitesse de libération*, Paris, Galilée, 1995.
 - WOJCIK S., *Prendre au sérieux la démocratie électronique. De quelques enjeux et controverses sur la participation politique en ligne*, in FOREY E., GESLOT C., (a cura di), *Internet, machines à voter et démocratie*, cit., pp. 111-141.

LA PROTEZIONE DEI DATI PERSONALI NELL'EVOLUZIONE NORMATIVA E GIURISPRUDENZIALE, EUROPEA E NAZIONALE. IL DIRITTO ALL'OBLIO

Sandro Di Minco

 *Multimedia*



Clicca sull'immagine o fotografa il QrCode
per accedere al MediaBook CLIOedu

DAL DIRITTO DI ACCESSO ALL'OPEN GOVERNMENT DATA: UN NUOVO PARADIGMA DI GESTIONE DEL PATRIMONIO INFORMATIVO PUBBLICO

Monica Palmirani

 *Multimedia*



Clicca sull'immagine o fotografa il QrCode
per accedere al MediaBook CLIOedu

**I NUOVI SCENARI DELLA SOCIETÀ
DELL'INFORMAZIONE: ASPETTI POLITICI,
GIURIDICI, AMMINISTRATIVI E TECNICI
CONCLUSIONI PRIMA PARTE**

Donato A. Limone

 *Multimedia*



Clicca sull'immagine o fotografa il QrCode
per accedere al MediaBook CLIOedu

INFORMATICA E DIRITTO TRA ANTINOMIE E ANALOGIE

Giancarlo Taddei Elmi

 *Multimedia*



Clicca sull'immagine o fotografa il QrCode
per accedere al Mediabook CLIOedu

Abstract: L'informatica e il diritto rappresentano l'ultimo anello di una relazione tra scienza giuridica e scienze esatte che risale nel tempo sin dal diritto romano. Nel corso del pensiero giuridico si sono avute oscillazioni tra concezioni formalistiche e concezioni storicistiche. Una analisi rigorosa delle fasi del processo "giuridico" come storia ideale della norma mette in luce omogeneità e resistenze tra diritto e informatizzazione. È analogica tutta quella parte del diritto morfo-sintattica riducibile a logica binaria mentre risulta antinomica tutta la parte semantica che richiede valutazione.

Parole chiave: informatica, diritto, teoria generale, scienza giuridica

Sommario: 1. A livello di contesti sociali; 2. A livello di contesti istituzionali; 3. A livello di contesti culturali generali; 4. A livello di contesti culturali giuridici; 4.1. A livello di teoria generale (essenza ed esistenza); 4.2. A livello di scienza giuridica; 4.2.1. ...di produzione della norma generale; 4.2.2. ...di elaborazione della norma generale come estensione semantica ed estensione logica; 4.2.3. ... di produzione della norma individuale; 4.2.4. Conclusioni relative alla elaborazione della norma generale e alla produzione della norma individuale

1. A livello di contesti sociali

L'Informatica e il Diritto appartengono per tradizione ad ambiti scientifici e disciplinari distinti, generalmente considerati incompatibili.

In realtà le interconnessioni tra questi due mondi sono più frequenti di quanto non si pensi. Nella storia del pensiero giuridico vi è sempre stata una oscillazione tra concezioni realiste-storicistiche e concezioni logico-formaliste. Molti sono gli approcci che hanno proposto l'uso delle scienze esatte nello studio e nella costruzione del diritto¹. Il rapporto tra informatica e diritto è l'ultimo stadio di un lungo percorso tra scienze formali e scienze giuridiche iniziato sin dal diritto romano. Tra informatica e Diritto, accanto ad aspetti certamente disomogenei e resistenti (antinomici) possono rinvenirsi aspetti omogenei e favorevoli (analogici).

Non ogni contesto sociale è tale da favorire lo sviluppo dell'informatica giuridica. Occorre in primo luogo che sia molto avanzato il processo stesso della giuridicizzazione. L'intero diritto oggettivo mostra una certa analogia di fondo con la visione cibernetica dell'uomo, può considerarsi come una specie di preparazione della realtà e dell'azione umana per tipi, ruoli, rapporti formali, quindi per fini di "sistemica" sociale paracibernetica; una società molto giuridicizzata si presta meglio a essere trattata algebricamente di una società poco giuridicizzata. Le società primitive, le comunità ferventi, anarchiche, spontaneiste, le società in fase di rivoluzione sono - a contrario - resistenti alla formalizzazione e all'informaticizzazione.

2. A livello di contesti istituzionali

All'interno del fenomeno della giuridicizzazione, può considerarsi particolarmente omogenea al

¹ D. Von Stephanitz, *Exakte Wissenschafts und Recht*, De Gruyter, Berlino, 1970.

pensiero calcolante e dunque all'informatica giuridica la struttura moderna dello Stato di diritto, inteso come Stato fondato sul principio del controllo del potere, particolarmente attraverso la razionalizzazione del sistema normativo al livello delle norme generali e la conseguente certezza delle situazioni giuridiche individuali.

Favorevolissimo all'informatica sembra invece lo Stato sociale pianificatore, che tende a sostituire lo Stato di diritto o a costituirne uno sviluppo e un'integrazione. In esso si verifica la giuridicizzazione tendenzialmente integrale dell'economia, della realtà in generale; norme giuridiche definiscono e regolano tutto il reale, un reale divenuto, da naturale, quasi integralmente artificiale. L'amministrazione complessiva del sistema società-natura porta un'estensione capillare del diritto pubblico e amministrativo, al sostituirsi del piano al codice come figura giuridica chiave. Questa enorme intrapresa di razionalizzazione calcolante genera i calcolatori elettronici che a loro volta la potenziano. L'uomo dei calcolatori è il nuovo consigliere del principe, un principe sempre meno personale, sempre più strutturale, anonimo: il Sistema. Tutto questo implica che il socialismo non rivoluzionario, la socialdemocrazia, possa considerarsi, ancora più del liberalismo sebbene in modi diversi e a volte opposti, omogeneo all'informatica giuridica.

Una ulteriore accentuazione dell'uso potenziale dell'informazione si riscontra nel modello tecnocratico, anche per la sua apparente almeno depoliticizzazione della politica, fondata sull'ideologia della fine delle ideologie. Qui il concetto limite è quello di legislazione (se non addirittura di politica o di amministrazione) automatica, come risultato di un puro calcolo razionale. Suprema realizzazione oggettiva dell'amministrazione sociale integrale va forse considerato lo Stato totalitario nella sua variante tecnoburocratica, perché il monismo ideologico consente di presumere il consenso generalizzato e quindi la pianificazione centralizzata di tutti senza eccezione gli aspetti della vita secondo criteri omogenei. Qui il "diritto" diviene esso stesso una sorta di "programma" (nel senso informatico) della storia, sia collettiva, sia individuale. L'informatica non favorisce necessariamente il totalitarismo: anzi certi suoi aspetti di modernità, efficienza, trasparenza dell'informazione gli resistono; ma un certo uso dell'informatica come potentissimo *instrumentum regni* troverebbe nella società totalitaria tecnoburocratica il suo luogo naturale. Che ciò di fatto non sempre avvenga è dovuto più che altro a transitori ritardi tecnologici

3. A livello di contesti culturali generali

Dal punto di vista culturale, è ovvio che l'informatica giuridica presuppone un generale orientamento verso lo scientismo tecnologico e verso le filosofie che lo sottendono o ne derivano, da Bacone, Galileo, Descartes in poi.

Tutti i metodi riduzionisti sono omogenei all'informatica giuridica. Tutte le logiche autentiche sono il presupposto di procedure algoritmiche che sono la base della informatizzazione della realtà. Il calcolatore è una macchina morfosintattica che riconosce significanti e sequenze di significanti ma non i significati. Presuppone elementi univoci veri o falsi. Trova resistenza in tutto ciò che è *fuzzy*, indefinito, semanticamente indeterminato².

² L. Lombardi Vallauri e G. Taddei Elmi, *Informatica, Società e Diritto*, relazione a Convegno "Potere informatico-Stato-

4. A livello di contesti culturali-giuridici

4.1. A livello di teoria generale

In teoria generale si distinguono teorie dell'essenza e teorie dell'esistenza del diritto. Le prime si occupano della ontologia del diritto, ossia di cosa è il diritto, le seconde della fenomenologia del diritto, ossia quale è il diritto vigente.

A livello di essenza sono analogiche tutte le teorie normative formalistiche, che definiscono il diritto come Legge dello Stato, come Comando della volontà sovrana (teoria imperativistica di Hobbes), come norma munita di sanzione, come norma prescrittiva (Kelsen). Mentre sono antinomiche le teorie del positivismo storicistico, del diritto come esperienza (Capograssi), come azione (Cotta, Piovanini), come rapporto (Santi Romano), come insieme di istituti che nascono per comportamenti ripetuti (Savigny).

Raggiunge il massimo della analogia la teoria dell'essenza che riduce il diritto a norme prescrittive del tipo se A allora B. Un tale *corpus* di norme costituisce la base più omogenea per la costruzione di un sistema informatico che intende elaborare la conoscenza in modo inferenziale.

In realtà questa teoria è molto parziale perché solo una minima parte degli enunciati normativi presentano una struttura prescrittiva. La maggior parte delle norme giuridiche sono semanticamente indeterminate nel senso della vaghezza e dell'ambiguità.

La legge è generale e astratta perché vi si possa ricomprendere il maggior numero di fattispecie possibili. Ciò rende necessaria una vasta opera interpretativa sia semantica che casistica. Tutto questo è altamente antinomico e resistente verso l'informatica.

A livello di vigenza sono analogiche tutte le teorie formaliste basate sul doppio postulato legalista "La legge è tutto il diritto e la legge è tutto diritto". Si esclude la consuetudine come fonte di produzione del diritto e la desuetudine come mezzo di abrogazione della legge. L'idea kelseniana che il diritto risiede solo nella legge posta da autorità legittima con procedure legittime è assolutamente pro-pre-informatica. Si raggiunge così il massimo grado di certezza del diritto vigente e applicabile. Tutto questo non può non favorire l'informatica sia documentaria sia decisionale che possono così basarsi su corpora normativi definiti.

Sono al contrario antinomiche tutte le teorie realiste: il diritto è quello osservato e applicato ossia effettivo (effettività di Alf Ross, scandinavi, americani, giurisprudenza interessi, scuola del diritto libero). Il diritto assume una veste meno definita e più aperta. L'individuazione delle norme vigenti in quanto osservate e applicate richiede un'opera anche sociologica che deve coinvolgere un sottile lavoro di analisi della giurisprudenza. Il giudice oltre che giurista deve assumere i panni del sociologo del diritto. Le applicazioni informatiche trovano in questa idea di diritto dinamico un forte ostacolo³.

Società, Erice, settembre 1987.

³ G. Taddei Elmi, *Informatica e filosofia del diritto*, in Atti del Congresso CED, Istituto poligrafico dello Stato, 1983.

4.2. A livello di scienza giuridica

Con scienza giuridica intendiamo l'insieme delle metodologie e delle tecniche dirette a produrre ed elaborare la norma generale (la legge) e a produrre la norma individuale (la sentenza). Per comodità sistematica utilizzeremo come schema di analisi le fasi dell'iter che la norma percorre dalla sua nascita fino alla sua applicazione concreta. Questo percorso ideale della norma che chiamiamo processo giuridico è scomponibile in tre grandi fasi: la produzione della norma generale o attività legislativa, la elaborazione della norma generale o attività dottrinarie e la produzione della norma individuale o attività giurisdizionale⁴.

4.2.1. ...di produzione della norma generale

L'iter di produzione della legge può essere scomposto almeno in cinque momenti: a) ricognizione del diritto vigente; b) scelta dei valori (momento assiologico); c) valutazione contesto sociale (momento sociologico); d) sintesi politica (momento politico) e e) la formulazione del testo legislativo (momento tecnico-giuridico).

a) Ricognizione diritto vigente

Il legislatore non opera in condizioni di tabula rasa. Ha davanti sempre un *corpus* normativo che già regola i vari aspetti della società. Modifica o integra un *corpus* normativo complesso e anche in questa prima fase il legislatore si deve comportare come il giurista-giudice nel momento in cui deve individuare il diritto vigente per poter decidere un caso concreto. Deve dunque fare una prima ricognizione del diritto vigente, perché prima di emanare una norma deve rendersi conto se la materia è già regolata esplicitamente o anche in via interpretativa. Sarebbe inutile creare una altra norma per regolare una materia già regolata. È il caso del diritto dell'informatica. Il legislatore prima di emanare una legge deve verificare che questa sia necessaria.

Un legislatore o accetta la teoria formalista o accetta la teoria dell'effettività o le accetta entrambe in modo complementare, ad esempio priorità della validità e primato della effettività. Perché se approva la teoria formale di Kelsen è semplice andare a capire quale è il diritto vigente perché va a vedere le leggi pubblicate sulla gazzetta ufficiale (archivi informatici delle norme formalmente poste); se invece è un effettivista guarderà non solo le leggi quindi il corpus normativo, ma dovrà occuparsi anche di altri archivi non solo delle norme formalmente poste ma anche archivi giurisprudenziali che raccolgono le applicazioni effettive delle norme e archivi di dati sociali che forniscono le osservanze da parte dei cittadini delle norme poste formalmente dal Parlamento. È qui che l'informatica si mostra analogica. Può aiutare il legislatore a consultare il diritto vigente formalmente posto ma anche il diritto vigente che è effettivamente applicato. A ciò risulteranno altamente utili le applicazioni dell'informatica documentaria (banche dati reali, virtuali e tutte le risorse informative della Rete. La prima informatica che interessa al legislatore è quella informativa, che raccoglie in banche dati il diritto vigente sia il diritto scritto pubblicato nella gazzetta ufficiale sia il diritto prodotto dai giudici.

⁴ L. Lombardi Vallauri, *Verso un sistema esperto giuridico integrale*, in Atti del venticinquennale dell'Istituto per la documentazione giuridica del CNR, Padova, Cedam, 1995.

b) Scelta dei valori (momento assiologico)

Questo secondo momento del legislatore è quello filosofico. Il legislatore una volta che ha fatto la ricognizione del diritto vigente, che ha verificato che vi è la necessità di creare una nuova norma, dopo aver consultato gli archivi informatici del diritto vigente, si pone un quesito di fondo chiamato filosofico, ossia il problema dei valori che intende tutelare attraverso questa nuova norma. (es: se devo fare una norma sull'inquinamento, e non vi sono norme applicabili a questa nuova fattispecie, si possono seguire due strade, una che tende a tutelare il bene della salute oppure tende a tutelare il bene della produzione industriale e cioè l'economia. Sono due valori costituzionali che possono essere tutelati in modo bilanciato da una normativa). Il momento filosofico è un momento chiamato assiologico cioè il legislatore si pone il problema di come orientare questa normativa, se nel senso di maggiore tutela della salute o dell'organizzazione industriale. Che può fare l'informatica per aiutare il legislatore in questa operazione? Può per esempio costruire delle indicazioni tenendo conto delle varie ideologie quindi può immaginare una legge orientata verso una applicazione liberista oppure più ecologica tipo "verde". Potrà fornire: o un ventaglio di proposte interlocutorie tratte da diversi sistemi assiologici (cattolico, personalista, liberale, socialista, verde, terzomondista; sistemi di singoli filosofi particolarmente autorevoli), oppure un'unica risposta definitiva ricavata, in base a un meta-programma, dal confronto tra i sistemi considerati. In questa fase l'informatica si presenta solo molto parzialmente omogenea e analogica al diritto perché potrà al massimo fornire delle indicazioni tra le quali il legislatore dovrà scegliere in maniera semantico-valutativa.

c) Valutazione contesto sociale (momento sociologico)

Dopo aver stabilito certi valori il legislatore si pone il problema di quale sarà l'impatto sulla società di questa nuova norma. E questo è il sociologo per il diritto. La differenza tra sociologo per il diritto e sociologo del diritto è che il sociologo per il diritto si pone il problema di quale sarà l'effetto della norma sulla società, il sociologo del diritto si pone il problema di verificare a posteriori gli effetti di una certa norma nella società. Il sociologo per il diritto potrà consultare anche dati di tipo fattuale per sapere se una norma è opportuna o meno e l'effetto di questa nella società. Per queste operazioni l'informatica documentaria appare molto analogica al diritto. Finita l'operazione del sociologo si passa attraverso un momento politico.

d) Sintesi politica (momento politico)

Il politico che comincia a delineare il testo della legge. Sarà un testo grezzo sulla base della sintesi del filosofo e del sociologo, che sarà poi consegnato ad un ufficio legislativo. Questa fase politica sarà permeata di opportunità e compromessi e poco spazio avrà lo strumento informatico.

e) Formulazione del testo legislativo (momento tecnico-giuridico)

Qui siamo nel momento finale della prima fase. E questo può chiamarsi momento legislativo in senso stretto, che ha un primo *step* che è costituito dall'ufficio legislativo. La tecnica giuridica è l'insieme di tutti quegli espedienti per rendere praticabile in concreto l'applicazione di una norma giuridica. Segnalo la riduzione del qualitativo a quantitativo (es: la norma che dice che la maggiore età si consegue a 18 anni è un assurdo dal punto di vista sostanziale). In molti casi la tecnica giuridica consiglia al legislatore di mettere dei dati quantitativi al posto della qualità, così che possa essere adoperata facilmente e di questo nel diritto vi sono molti esempi.

Poi si procede alla redazione formale del testo che deve essere con un linguaggio chiaro e anche una struttura logica formale e deve essere coerente. Un modo di fare delle leggi secondo un

criterio standard. Tanto è che il giurista Simitis negli anni '70 propose un disegno di legge in cui suggeriva dei criteri per rendere informaticizzabili le leggi⁵. In realtà questa raccomandazione non è stata molto seguita.

Le regole della tecnica giuridica sono proinformatiche. L'informatica stessa offrirebbe strumenti così detti legimatici per aiutare la formulazione e la redazioni di leggi coerenti dal punto di vista sostanziale e formale.

4.2.2. ... di elaborazione norma generale

Il giurista si trova sul tavolo da un lato il corpus normativo formalmente prodotto da legislatore e dall'altro il caso concreto da risolvere attraverso una sentenza, un parere, una norma che Kelsen chiama individuale.

Ma prima di poter intraprendere le operazioni strettamente decisionali deve porsi almeno due grandi compiti a) stabilire all'interno di quel *corpus* normativo quale diritto è veramente vigente ossia applicabile e b) se quel diritto vigente consente di poter prendere una decisione, ossia se il caso che ha di fronte è regolato da quel *corpus* normativo. Queste operazioni di riconoscimento del diritto vigente presentano subito difficoltà. Anche partendo dal postulato legalista, il testo che ho di fronte non è tutto vigente perché deve essere depurato da tutti gli interventi di abrogazione, modifica, aggiunta etc. Questi possono essere espliciti ma anche taciti e impliciti. L'informatica risulta essere decisiva nell'individuare l'esplicito e così nel redigere testi coordinati vigenti ma nulla può fare verso l'implicito e il tacito. Qui è necessaria l'opera interpretativa del giurista o del giudice. Una prima operazione *sub a)* che il giurista-giudice deve compiere è la individuazione e risoluzione delle antinomie tra norme.

Le antinomie sono situazioni o enunciati normativi incompatibili e si distinguono in proprie e improprie. Si dicono norme antinomiche proprie quelle per cui vale la regola che non possono essere entrambe vere. Ad esempio una norma che obbliga e una norma che vieta il medesimo comportamento (caso di contrarietà) . Oppure una norma che obbliga e una che permette (contraddittorietà), oppure una norma che vieta e una norma che permette (contraddittorietà). Si tratta di incompatibilità logiche o assolute.

Le antinomie proprie ossia norme incompatibili che non possono essere entrambe vere possono essere risolte con dei criteri forniti dalla scienza giuridica ma non tutte.

Per cui distinguiamo tra antinomie solubili o apparenti e antinomie insolubili o reali. Le antinomie apparenti sono quelle solubili con i criteri formali, cronologico (*lex posterior derogat priori*), gerarchico (*lex superior derogat inferiori*) e di specialità (*lex specialis derogat generali*).

Tutto ciò è altamente omogeneo all'informatica che riuscirà agevolmente ad individuare e a risolvere questo tipo di incompatibilità normativa attraverso procedure automatiche. Siamo di fronte a elementi binari, vietato-obbligatorio, norma precedente-norma-successiva e così via.

Vi sono però dei casi in cui i criteri o non sono sufficienti o sono in conflitto. Non sono sufficienti ad esempio nel caso di norme contemporanee, sullo stesso livello o rango e entrambe generali.

⁵ S. Simitis, *La crisi dell'informazione giuridica*, Giuffrè, Milano, 1977.

Non si può applicare alcun criterio. Vi sono dei criteri non vincolanti, fondati sulla forma della norma, su cui basare la prevalenza: la permissiva potrebbe prevalere come *favorabilis* sulla obbligatoria e di divieto (criterio labile e non sempre applicabile) e nel caso di incompatibilità-contrarietà (obbligatorio-vietato) far prevalere il *tertium* ossia il permesso.

Le soluzioni potrebbero essere a) eliminare una delle due norme b) eliminarle entrambe o c) conservarle entrambe dimostrando la non incompatibilità attraverso una interpretazione che Bobbio chiamava correttiva. È una forma di bilanciamento *ante litteram*?

In caso di conflitto tra criteri prevale il criterio più forte (gerarchico e di specialità rispetto al cronologico). Ma se il conflitto è tra criteri forti ad es. tra *superior generalis* e *inferior specialis*, quale prevale? Il conflitto in questo caso si risolve con soluzione interpretativa a seconda delle circostanze. Di fronte a queste ipotesi di antinomie reali insolubili con i criteri formali l'informatica non può fare nulla⁶.

Si dicono invece improprie quelle antinomie per cui non vale la regola della incompatibilità logica assoluta. Si tratta di norme in conflitto relativo nel senso che possono essere entrambe vere a seconda delle situazioni. Di questo tipo di antinomie è piena la nostra costituzione e mi riferisco alle norme che affermano principi, valori, esigenze quali ad esempio la tutela della salute, del lavoro, dell'ambiente, della sicurezza collettiva, della libertà individuale, dell'iniziativa economica, etc. Come è evidente siamo di fronte a norme che possono essere entrambe vere.

In questi casi si deve ricorrere a metodi interpretativi fondamentali e sistematici per bilanciare le applicazioni di queste norme che possiamo chiamare a efficacia graduale. Ed è altrettanto evidente che l'informatica trova resistenza forte in questo tipo di operazioni.

Il giurista-giudice dopo aver individuato il diritto vigente applicabile e aver eliminato le antinomie passa alla fase *sub b)* ossia quella in cui si deve verificare la sufficienza del diritto vigente per risolvere il caso concreto. Ci si imbatte nel fenomeno delle lacune che risulta essere più ampio di quanto non ci si aspetti. Alcuni dicono che il diritto è un arcipelago dove le norme sono le isole e il mare le lacune. Legalisti e non legalisti ammettono entrambi l'esistenza di lacune ma è nella ricetta per riempirle che divergono fortemente. I primi sostengono che il sistema è autocompletabile con operazioni logiche senza necessità di alcun intervento integrativo valutativo esterno sia del giurista (elaborazione dottrinale) sia del giudice (interpretazione giurisprudenziale). E in proposito avanzano molti espedienti tra cui la negazione logica delle lacune, l'analogia, la costruzione dogmatica, gli argomenti *a fortiori*, etc. I non legalisti, al contrario, ritengono che sia inevitabile ricorrere a metodi valutativi (interpretazioni) e che anche i cd. metodi logici suggeriti dai legal-logicisti non sono logici autentici e nascondono al loro interno un momento semantico.

La negazione logica delle lacune basata sulle due norme generali di chiusura "tutto ciò che non regolato è irrilevante" o "ciò che non regolato è permesso" sono state oggetto di forti critiche perché la prima condurrebbe per il divieto del *non liquet* a decidere a caso o tirando a sorte mentre la seconda più solida risolverebbe esclusivamente le lacune assolute e non quelle relative e comporterebbe molte norme consequenziali del tipo "sono vietate tutte le azioni in contrasto con il comportamento permesso". Altro che norma di chiusura!

L'analogia consistente nell'estrazione di un principio da una norma e l'estensione a un caso non regolato non sarebbe altro che una interpretazione fondamentale. Negli argomenti *a fortiori* affermare

⁶ N. Bobbio, *Teoria dell'ordinamento giuridico*, Giappichelli, Torino, 1960.

che un diritto è *minus* o *maius* rispetto a un altro è una valutazione semantica che inficia tutto il sillogismo conseguente. È necessario ricorrere a metodi valutativi, semantici come l'interpretazione. I metodi interpretativi sono molteplici e valutativa è sia la loro scelta sia la selezione tra i risultati possibili di ciascun metodo.

Ad esempio di fronte anche alla banale norma vietato introdurre cani si può optare per il metodo letterale e il metodo fondamentale (*ratio*) con ovvi risultati diversi; e una volta scelto il fondamentale (concettuale) vietato introdurre animali *tout court* arriverò a un certo risultato per cui nessun animale entra, oppure se scelgo quello fondamentale teleologico (il fine) posso individuarlo o nell'occupazione dello spazio (e allora il canarino entra e l'elefante no) oppure nella tutela della salute (e allora non entra l'animale malato) e così via. L'informatica può al massimo fornire ventagli di possibili soluzioni tante quante sono le possibili interpretazioni.

Terminata la fase di estensione semantica della norma generale con una scelta ad esempio di interpretazione fondamentale concettuale che ci conduce a una norma generale estesa tipo "Vietato introdurre animali" è possibile sviluppare una estensione logica della norma generale utilizzando strumenti logici autentici quali il sillogismo. La norma generale "Vietato introdurre animali" può rappresentare la premessa maggiore da cui partire. Se la premessa minore fosse "I cani sono animali" si potrebbe giungere a una conclusione corretta e certa e vera in base alla certezza e verità della premessa, "i cani non possono entrare"

La regola sillogistica ipotetica che sta alla base di una estensione logica della norma generale potrebbe essere la seguente:

*"Se gli animali non possono entrare
e x è un animale
allora x non può entrare"*

La norma generale dunque si presenta con tutta una serie di sillogismi incorporati.

Siamo quindi giunti a determinare la portata della norma generale attraverso due grandi operazioni intellettuali, una semantica, con la quale abbiamo reso univoco il significato dell'enunciato, e una logica, con la quale abbiamo creato un grappolo di implicazioni logiche possibili agganciate all'enunciato univoco di base.

L'esempio: "vietato introdurre cani" è diventato in base alla prima operazione di estensione semantica "vietato introdurre animali" (interpretazione fondamentale concettuale). Operazione questa fortemente antinomica nei confronti dell'informatica.

Con la seconda operazione estensiva, quella logica, ho integrato la norma base con una serie di possibili implicazioni implicite. Per esempio "se x è un serpente e se un serpente è un animale allora il serpente non entra" e così via per il pappagallo, per l'orso, etc.

Questa seconda operazione è altamente omogenea rispetto all'informatica. Il calcolatore può agevolmente eseguire implicazioni logiche di questo tipo.

4.2.3. ... di produzione della norma individuale

Con norma individuale si intende la soluzione di un caso attraverso la sentenza, il lodo arbitrale, il parere legale etc. Si tratta di confrontare la fattispecie con la fattispecie astratta emersa dalla fase di

elaborazione norma generale. La fattispecie concreta Fido (cane) che entra nella sala è facilmente comparabile con la fattispecie astratta prevista dalla norma.

Si realizza una sussunzione della fattispecie concreta nella fattispecie astratta. L'individuazione di Fido come animale può realizzarsi attraverso il confronto con un modello (*frame*) di animale costituito da elementi necessari e sufficienti per individuare la classe. Il confronto del modello con l'individuo consente di controllare automaticamente se le condizioni sono verificate. Una volta accertata la natura di animale di Fido sono in grado di attivare un altro sillogismo:

“Vietato introdurre animali

Fido è un animale

Fido non entra”

Ho prodotto automaticamente la norma individuale. Dunque tutte le operazioni della produzione della norma individuali sono teoricamente informaticizzabili anche se richiedono un grosso lavoro di rappresentazione della conoscenza zoologica. Un sistema di riconoscimento automatico dell'entità X (Fido) può agevolmente consultare un mega-archivio zoologico e decidere logicamente (=informaticamente) il caso. “Se Fido è un animale Fido non entra”, questa è la semplice conclusione di un giudice-robot. La difficoltà è nel lavoro di rappresentazione di tutta la conoscenza necessaria non nella operazione di utilizzo di questa conoscenza.

4.2.4. Antinomie e analogie relative alla elaborazione della norma generale e alla produzione della norma individuale

Per concludere possiamo dire che sono operazioni non informaticizzabili:

1. il riconoscimento diritto vigente: “vietato introdurre cani”;
2. la valutazione della lacuna (l'entità che si presenta è un animale ma non un cane) che necessita di riempimento con metodi non logici;
3. la scelta “politica” del metodo interpretativo: ad es. fondamentale concettuale piuttosto che altri;
4. l'estensione semantica della norma generale: “ vietato introdurre animali”.

Sono invece informaticizzabili:

1. l'estensione logica della norma generale attraverso l'applicazione del sillogismo con premessa maggiore “vietato introdurre animali” predeterminata in via interpretativa e premessa minore “entità (X) è un animale” con conclusione “X non entra”;
2. la produzione della norma individuale attraverso la verifica della situazione concreta (Fido è un animale) con tecniche di confronto e applicazione sillogismo finale⁷.

⁷ G. Taddei Elmi, *Corso di informatica giuridica*, Simone, Napoli, 2010.

LO STATO E LE SUE BUROCRAZIE DIGITALI

Pasquale Luigi Di Viggiano

 *Multimedia*



Clicca sull'immagine o fotografa il QrCode
per accedere al Mediabook CLIOedu

Abstract: L'evoluzione dello Stato moderno si può rappresentare attraverso l'analisi delle sue burocrazie. Osservare lo sviluppo della Società dell'informazione dal punto di vista della progressiva digitalizzazione dello Stato e dei suoi apparati rappresenta un'utile approccio per richiamare

e descrivere le acquisizioni e le sedimentazioni tecnologiche, giuridiche e organizzative che realizzano le attuali burocrazie digitali come enti operativi dello Stato. L'idea secondo la quale la società moderna contemporanea è l'universo della comunicazione sociale si coniuga perfettamente con l'indicazione che individua l'attuale società come "Società dell'informazione e della comunicazione". Quindi, la comunicazione e le pratiche sociali, tecniche, organizzative, economiche e politiche che la rendono possibile, rappresentano il riferimento verso il quale si orientano le reti telematiche e i contenuti digitali attraverso queste veicolati. In questo scenario possiamo individuare le pratiche dello Stato, considerato come un ordinamento giuridico-politico che a fini generali esercita il potere sovrano su un determinato territorio e sui soggetti a esso appartenenti, attraverso le quali si organizza per esercitare il proprio potere e che rendono possibile la partecipazione democratica dei cittadini.

The evolution of the modern State can be represented through an analysis of its bureaucracies. By observing the development of the information and communication society from the point of view of the progressive digitization of the State and its apparatuses we can thus describe the acquisition and technological, legal and organizational sedimentations that realize the current digital bureaucracies such as operating State apparatuses. The idea according to which the contemporary modern society is the universe of social communications is perfectly matched with the indication that locates the current society as an "information and communication Society". Therefore, communication and social practices, (technical, organizational, economic and political) that make the communication society possible, are the reference points from which computer networks and the production of digital content that they themselves conveys. In this scenario, we can identify the practices of the State, and consider them as legal and political frameworks for general purposes that exercise sovereign power over a certain territory and the people belonging to it. We can examine how they exert their power thus making the democratic participation of citizens possible.

Parole chiave: Stato digitale, Stato virtuale, e-Democracy, Burocrazie digitali, Società dell'informazione e della comunicazione, Controllo sociale, e-Government.

Sommario: 1. Premessa - 2. Lo Stato e la Società dell'Informazione - 3. La costruzione delle burocrazie digitali - 4. La comunicazione digitale dello Stato moderno - 5. Conclusioni - Bibliografia.

1. Premessa

Una delle linee di ricerca adottate dal Laboratorio di eGovernment (LEG) dell'Università del Salento e dall'ANDIG di Lecce riguarda lo studio del rapporto tra lo Stato e le sue burocrazie sempre più digitali. L'idea secondo la quale la società moderna contemporanea è l'universo della comunicazione sociale¹ si coniuga perfettamente con l'indicazione che individua l'attuale società come "Società dell'informazione e della comunicazione". Quindi, la comunicazione e le pratiche sociali, tecniche, organizzative, economiche e politiche che la rendono possibile, rappresentano il

¹ Cfr. N. Luhmann, R. De Giorgi, *Teoria della società*, Franco Angeli, Milano 1992.

riferimento verso il quale si orientano le reti telematiche e la produzione di contenuti attraverso queste veicolati.

Il questo scenario osserviamo come lo Stato², considerato come un ordinamento giuridico-politico che a fini generali esercita il potere sovrano su un determinato territorio e sui soggetti a esso appartenenti, si organizza per esercitare il proprio potere sia nella sua forma di Stato-comunità, formato dal popolo, stanziato su un determinato territorio, organizzato attorno a un potere centrale (comunemente chiamato “Stato-nazione”) sia nella sua forma di Stato-apparato (o Stato-organizzazione) rappresentato dal potere centrale sovrano, stabile nel tempo e impersonale (poiché esiste indipendentemente dalle singole persone che lo fanno funzionare), organizzato in possibili differenti modi, che detiene il monopolio della forza e impone il rispetto di determinate norme nell’ambito di un territorio ben definito.

Lo strumento che lo Stato utilizza per l’esercizio delle proprie funzioni è rappresentato dalle burocrazie ai vari livelli stabilite.

Con l’affermarsi degli strumenti che connotano la società dell’informazione e della comunicazione, in particolare le ICT, l’esercizio del potere statale tramite gli apparati burocratici, dapprima timidamente poi in maniera progressivamente pervasiva, si avvia ad essere sempre più automatizzato, tecnologicamente organizzato; sempre più digitale, sempre più *smart*. La digitalizzazione delle burocrazie è un processo in fieri, che registra accelerazioni che descrivono livelli di sviluppo mai finora osservati.

Agli inizi del nuovo millennio si parla sempre più spesso di gestione elettronica delle attività di governo ad ogni livello e comincia ad affermarsi un sistema di gestione digitalizzata della pubblica amministrazione. Questo sistema - unitamente ad azioni di cambiamento organizzativo - consente di trattare la documentazione e di gestire i procedimenti con sistemi informatici, grazie alle ICT, allo scopo di ottimizzare il lavoro degli enti e di offrire agli utenti (cittadini ed imprese) sia servizi più rapidi, che nuovi servizi sul versante della comunicazione telematica. Parliamo di eGovernment, ancora con un approccio generalista, ma la tappe segnate dal diritto e dall’organizzazione della PA, a partire dall’EU e proseguendo in ambito nazionale, progressivamente affinano le buone pratiche e perfezionano le norme in senso digitale. Questo consente di superare l’approccio generalista e pertanto, attraverso un processo di differenziazione funzionale, è possibile registrare sempre nuove specificità di governo elettronico, fino a individuarne ambiti specifici: e-Government, eHealth, eJustice, eDemocracy, eProcurement, con in dotazione un correlato di esclusione/inclusione rappresentato dal digital divide.

Parallelamente, le tecnologie della comunicazione a disposizione del potere statale ed economico consentono e producono un controllo totale sulla comunicazione, e quindi sulla società, che alcune proiezioni letterarie definite “distopiche” avevano già individuato nella descrizione delle società

² Cfr. A. Mattioni, F. Fardella, *Teoria generale dello Stato e della Costituzione. Un’antologia ragionata*, Giappichelli, Torino 2009; J. H. Shennan, *Le origini dello stato moderno in Europa*, Il Mulino, Bologna 1991.

del futuro. La metafora del *Panopticon* di Bentham³ e il più celebre *Big Brother* di Orwell⁴ rappresentano le istanze più popolari di questa visione apocalittica.

Osservare lo sviluppo della società dell'informazione dal punto di vista della progressiva digitalizzazione dello Stato e dei suoi apparati rappresenta un'utile approccio per richiamare e descrivere le acquisizioni e le sedimentazioni tecnologiche, giuridiche e organizzative che rendono possibili le attuali burocrazie digitali come apparati operativi dello Stato.

2. Lo Stato e la Società dell'Informazione

Le forme contemporanee dello Stato continuano ad evolversi mantenendo la caratteristica della modernità intesa come capacità di differenziazione delle proprie funzioni anche quando si considerino gli aspetti più innovativi delle tecnologie comunicative fino a parlare di Stato Virtuale⁵ o di Stato Digitale⁶.

La letteratura scientifica finora prodotta ha affrontato il tema dello Stato, che sempre più utilizza le tecnologie dell'informazione e della comunicazione (ICT), con approcci settoriali: politologici, economici, giuridici, sociologici, tecnologici, senza mai proporre una visione d'insieme in cui la virtualizzazione, o meglio la digitalizzazione, riguardi gli apparati, ma anche gli influssi che continuamente contribuiscono a modificare l'idea delle componenti classiche costitutive dello Stato moderno: il popolo, il territorio e la sovranità⁷.

L'obiettivo del presente intervento è tracciare un percorso di riflessione che consideri alcuni macro-elementi costituenti la società e lo Stato moderno nell'intento di osservare e descrivere come l'ordinamento giuridico si modifica quando impatta con le ICT, come queste contribuiscono a modificare in senso digitale lo Stato e le sue burocrazie e come tutto ciò consente alla società di esercitare meglio diritti acquisiti e costituire presupposti per nuovi diritti.

L'approccio verso una visione di Stato digitale è rivolto soprattutto verso un sistema di comunicazione elettronica che ha un linguaggio comune ormai universale e che è rappresentato dal codice

³ Cfr. J. Bentham, *Panopticon ovvero la casa d'ispezione* (a cura di M. Foucault e M. Pierrot), Marsilio, Venezia 1983. [Ed. originale: *Panopticon or the inspection-house*, T. Payne, London 1791]. Bentham progetta questo metodo di controllo applicabile sia alle prigioni che alle fabbriche. In riferimento alla prigione, l'idea alla base del Panopticon ("che fa vedere tutto") era quella che - grazie alla forma radiocentrica dell'edificio e ad opportuni accorgimenti architettonici e tecnologici - un unico guardiano potesse osservare (optikon) tutti (pan) i prigionieri in ogni momento, i quali non devono essere in grado di stabilire se sono osservati o meno, portando alla percezione da parte dei detenuti di un'invisibile onniscienza da parte del guardiano, che li avrebbe condotti ad osservare sempre la disciplina come se fossero osservati sempre. Amplificata, questa idea si connota come presupposto per il controllo sociale totale.

⁴ Cfr. G. Orwell, *1984*, Arnoldo Mondadori Editore, Milano 2000. Nel 2013 è stato il romanzo dell'estate. Questo perché, dopo che è iniziato lo scandalo DATAGATE legato al sistema di analisi dei dati e delle telefonate PRISM elaborato dalla NSA, l'agenzia di sicurezza nazionale Usa, Amazon ha registrato un aumento delle vendite del 7000 per cento. Lo scandalo "Prism", ha fatto scattare la paura di una società ipercontrollata.

⁵ Cfr. J. E. Fountain, *Building the virtual State: Information Technology and Institutional Change*, Brookings Institution Press 2001.

⁶ Cfr. F. Bollorino, A. Rubini, *Ascesa e caduta del terzo stato digitale. Un promemoria politico per il terzo millennio*, Apogeo, Milano 1999.

⁷ Cfr. H. Kelsen, *Teoria generale del diritto e dello Stato*, Etas, Milano 2009.

binario. La costruzione di applicazioni istituzionali rappresenta la modalità attraverso la quale si costruiscono i diversi sistemi informativi che costituiscono un insieme coordinato di assetti organizzativi, tecnologici, logistici, strumentali e, non da ultimo, di risorse umane specificamente formate.

Per il controllo del territorio, per l'acquisizione e la gestione del consenso, nonché per l'esercizio della sovranità sono disponibili ormai da tempo tecnologie digitali sempre più raffinate ed efficaci e norme giuridiche e commerciali che consentono allo Stato di operare in maniera difforme rispetto al passato e con un approccio impensabile solo 20 anni fa.

Il contributo del digitale per il monitoraggio e il controllo del territorio annovera oggi numerosi strumenti che svolgono funzioni fondamentali, se adottati, per creare una rappresentazione digitale del territorio, mapparlo in base a indicatori predefiniti, intervenire puntualmente in caso di necessità. La creazione e la gestione di database di ultima generazione consentono un'acquisizione di dati, la loro elaborazione e conservazione in base alle esigenze dello Stato con il supporto di tecnologie performanti, di norme giuridiche specifiche e di standard tecnici condivisi e approvati. Gli strumenti operativi sono rappresentati dalla georeferenziazione satellitare, dall'uso di droni, da sistemi di videosorveglianza diffusi e, non da ultimo, da applicazioni professionali di Google heart⁸. I cosiddetti sistemi informativi geografici per il governo del territorio, indifferentemente citati come SIT o GIS (Geographic Information System), e si occupano di trattare dati geografici e metadati in riferimento a informazioni spaziali o informazioni non spaziali. Le informazioni di questo tipo sono alla base della costruzione di cartografie digitali a 2 o a 3 dimensioni e che a livello diacronico rappresentano la mutevolezza nel tempo del territorio. Le informazioni geografiche trattate in questa maniera possono rappresentare per gli enti governativi un'utile possibilità per la pianificazione dei processi decisionali e delle risorse ambientali⁹, oltre che un controllo puntuale delle attività antropiche.

L'influenza delle tecnologie della SI e la parallela riorganizzazione delle burocrazie ha consentito di intervenire con sempre maggiore efficacia nella progressiva digitalizzazione delle strutture amministrative che rendono possibile l'esercizio dei diritti di cittadinanza e la realizzazione di strutture tecnologicamente e organizzativamente avanzate per la gestione del Welfare¹⁰. Assistiamo così a interventi atti non a cambiare le regole democratiche, ma a renderle applicabili per una virtuale partecipazione di tutti i cittadini. Parliamo allora di eVoting¹¹, per consentire un accesso più diffuso e sicuro agli strumenti per l'esercizio del diritto di voto; la rete diventa l'arena del confronto

⁸ Google Earth è un software che genera immagini virtuali della Terra utilizzando immagini satellitari ottenute dal telerilevamento terrestre, fotografie aeree e dati topografici memorizzati in una piattaforma GIS. Il programma è distribuito gratuitamente dalla società Googlem a esiste anche una versione professionale. Inizialmente il programma si chiamava Keyhole ed era sviluppato dalla Keyhole, inc. ma nel 2004 la società venne acquisita da Google e il software rinominato di conseguenza. Richiede un sistema operativo Microsoft Windows, Mac OS X o Linux e recentemente Google ne ha sviluppata una versione per telefoni cellulari basati su piattaforma Android e iOS. http://it.wikipedia.org/wiki/Google_Earth.

⁹ L. Buccoliero, *Il Governo elettronico. Modelli, strategie di innovazione ed elementi di valore per una pubblica amministrazione digitale*, Tecniche nuove, Milano 2009, p. 151 e ss..

¹⁰ Cfr. C. Saraceno, *Il Welfare. Modelli e dilemmi della cittadinanza sociale*, Il Mulino, Bologna, 2013.

¹¹ Il progetto *Salento eVoting*, coordinato dal prof. Mancarella e promosso dal *Laboratorio di eGovernment* dell'Università del Salento, in collaborazione con ANDIG, rappresenta oggi il tentativo più avanzato di voto elettronico sperimentato con successo in diversi Stati. Cfr. <http://www.salentoevoting.it/>.

democratico per il confronto politico diffuso finalizzato alla ricerca del consenso; la partecipazione del cittadino alla *res publica* passa sempre più frequentemente attraverso la comunicazione telematica istituzionale. L'esercizio della sovranità dello Stato, comunque intesa, transita attraverso le dorsali della rete globale con una velocità e una tempestività finora relegate nella letteratura fantascientifica.

3. La costruzione delle burocrazie digitali

Il processo di costruzione dello Stato digitale e lo sviluppo della informatizzazione delle sue burocrazie è stato segnato da diverse importanti *miles stone*: alcune di natura tecnologica, altre di natura giuridico-organizzativa, altre ancora riferibili a programmi di governo.

L'avvento delle tecnologie informatiche e telematiche ha rivoluzionato non solo le scienze esatte, ma anche quelle della sfera umanistica. Gli effetti di questa nuova applicazione delle ricerche fisico-matematiche chiamata informatica mentre sono ben visibili se consideriamo gli aspetti economici e la riprogrammazione della produzione industriale e ingegneristica, altre discipline come ad esempio l'istruzione, la medicina, il diritto, la politica, l'osservazione della società e della psiche, hanno tardato a confrontarsi con questa tecnologia digitale che, attualmente, si sta imponendo come pervasiva. L'hardware e il software, le reti di comunicazione e le tecnologie di connessione ad Internet, i nuovi modelli di comunicazione sociale e istituzionale rappresentano le acquisizioni che sono poste alla base della società dell'informazione la quale assume sempre più una portata universale.

L'idea che fosse possibile una proficua contaminazione fra le scienze esatte e le scienze rigorose, in particolare il diritto, rappresenta la prima riflessione su cui Loevinger nel 1949¹² pone i presupposti di una nuova scienza, che aveva battezzato «jurimetrics» (giurimetria) per definire l'utilizzazione dei metodi delle scienze esatte e in particolare dell'informatica nel campo del diritto.

Loevinger auspicava l'uso metodico dell'informatica per aiutare e verificare le scelte legali, partendo dall'applicazione delle leggi antitrust, anche per elaborare in modo efficiente l'enorme massa di dati economici che le agenzie statali dovevano analizzare per accertare agevolmente eventuali posizioni dominanti di determinate imprese nel mercato. I bit diventano i piccoli mattoni su cui si cominceranno a costruire le burocrazie digitali, su cui poggerà l'intera società dell'informazione.

Nel 1970, in Cile, la Coalizione di *Unidad Popular* portò alla carica di Presidente Salvador Allende sostenendo un programma politico che prevedeva, tra l'altro, la nazionalizzazione dei settori centrali dell'economia cilena, per porre fine al potere del capitale monopolistico nazionale e straniero del latifondo. In questa nuova visione dell'economia nazionale cilena ebbe un ruolo importantissimo la pianificazione gestita e realizzata dagli organi dell'Amministrazione statale che avevano carattere esecutivo. Il vasto processo di nazionalizzazioni e di espropri che seguirono all'insediamento di Allende diede vita a un'area pubblica di grandi dimensioni nell'economia: la cosiddetta "Area Sociale".

I problemi organizzativi e manageriali derivanti dalla programmazione, direzione e gestione

¹² Cfr. L. Loevinger, *Jurimetrics. The Next Step Forward*, Minnesota Law Review, 1949.

dell'Area Sociale apparvero presto in tutta la loro complessità. Fu allora che il governo cileno decise di dar vita ad un progetto di ricerca che definisse un modello di governo dell' Area Sociale, considerandola come un sottosistema all'interno della società cilena, con specifici problemi di comunicazione e di controllo.

Questo progetto che doveva sperimentare “come la cibernetica può essere usata nell'esercizio del governo della nazione”¹³ fu condotto da una dozzina di giovani ricercatori e di manager cileni diretto da Stafford Beer. Ad esso fu dato nome Cybersyn passando ben presto da “strumento tecnico, per scopi amministrativi” a sistema determinante per la gestione del paese¹⁴.

“Il punto di vista centrale di Cybersyn è riassunto nel suo stesso nome, contrazione di cybernetics e synergy. Dalla cibernetica esso prende l'enfasi nel considerare la totalità di un sistema: la sua struttura, la sua dinamica e il rapporto tra controllo, informazione, pianificazione e decisione. Il concetto di sinergia è sottolineato in quanto efficienza e rendimento dovrebbero essere messi in relazione con l'effetto moltiplicante dato dagli opportuni legami di cooperazione tra i diversi elementi, piuttosto che da regolazioni astratte e formali imposte al sistema dall'esterno”¹⁵. Nel giugno 1973 un nuovo sciopero degli autotrasportatori cileni diede inizio ad una nuova offensiva reazionaria, che doveva concludersi con il golpe di Pinochet. “L'11 settembre 1973 i piani erano quasi pronti [per l'attuazione del progetto Cybersyn] ma il palazzo della Moneda stesso fu ridotto a fumanti rovine”¹⁶.

È il primo tentativo di applicare in maniera sistematica alla gestione di uno Stato le nuove tecnologie, ancora immature ma di grande portata, che aprivano una timida finestra sul futuro della gestione non solo degli Stati e delle loro burocrazie, ma di tutta la società contemporanea.

Nel governi di tutto il mondo, non solo occidentale, i politici vedono Internet sia come una forza per incrementare la reattività del governo verso i suoi cittadini sia come mezzo per potenziare ulteriormente lo stato. Nei paesi in via di sviluppo, le nuove tecnologie dell'informazione e della comunicazione *online* segnalano un'opportunità senza precedenti per accelerare il ritmo di sviluppo e di collegamento con il mondo sviluppato. Un marcato aumento della crescita dei sistemi sociali - finanziari, legali e normativi transnazionali ha sollevato un dibattito serio su Internet circa il futuro, la posizione e le strutture di governance. Nei regimi autoritari Internet minaccia il dominio da parte dello Stato sulla informazione e sulla comunicazione, ma allo stesso tempo, paradossalmente, serve come strumento di sorveglianza dello stato e di controllo sulla società¹⁷.

Nel 1993 è iniziata una fase fondamentale della crescita impressionante di Internet verificatasi in coincidenza con il periodo iniziale di un grande sforzo di riforma del governo statunitense, il *National Performance Review*, guidata dal Vice Presidente Al Gore. Avendo concentrato l'attenzione inizialmente sullo sviluppo di regimi normativi e giuridici volti a favorire l'e-commerce, successivamente il Governo rivolse i suoi sforzi verso il compito di costruire il governo digitale attraverso

¹³ S. Beer, *Fanfara per una libertà efficace: la prassi cibernetica nell'esercizio del governo*, in AA:VV., *Il progetto Cybersyn. Cibernetica per la democrazia*, (A cura di F. De Cindio e G. De Michelis), CLUP-CLUED., Milano 1980, pag. 113 e ss.

¹⁴ R. Espejo, *La prassi cibernetica nell'esercizio del governo: la gestione dell'industria in Cile*, in AA:VV., *Il progetto Cybersyn. Cibernetica per la democrazia*, cit., p. 323.

¹⁵ H. Schwember, *Il progetto Cybersyn: nuovi strumenti per la gestione nell'esperienza cilena*, in AA:VV., *Il progetto Cybersyn. Cibernetica per la democrazia*, cit., p. 229.

¹⁶ S. Beer, *Cibernetica dello sviluppo nazionale sulla base dell'esperienza vissuta in Cile*, in AA:VV., *Il progetto Cybersyn. Cibernetica per la democrazia*, cit., pag. 181.

¹⁷ Cfr. J. E. Fountain, *Introduction*, in “*Building the virtual State: Information Technology and Institutional Change*”, cit., p. 3 e ss..

la strategia di creazione di *Agenzie virtuali*. L'Agenzia virtuale, seguendo il modello dei portali web utilizzati per l'economia, è organizzata da client - per esempio, studenti, pensionati, piccoli imprenditori, o veterani. Ogni sito è progettato per fornire tutti i servizi e le informazioni del governo attraverso qualsiasi agenzia così come i collegamenti alle organizzazioni non governative più importanti. I portali web, estendendo al governo il concetto di business secondo il modello di 7 x 24 x 365 (essendo disponibile sette giorni su sette, 24 ore al giorno, 365 giorni l'anno), contribuiscono a riformare il rapporto tra Stato e cittadino rendendolo più semplice, più interattivo e più efficiente.

Uno Stato virtuale (il termine è di J. Fountain) è un governo che si organizza sempre più in termini di agenzie virtuali, di enti intermedi e di reti pubblico-privato la cui struttura e capacità dipendono da Internet e dal web¹⁸.

Nei primi anni novanta del secolo scorso la Comunità europea ha iniziato a porre le prime fondamenta per una società digitale. Si iniziano a definire le prime regole comuni per l'applicazione di strumenti informatici all'interno dello Stato-apparato, inizia a cambiare la mentalità e la concezione del modo di fare "burocrazia" all'interno della stessa Europa. Si tende, dunque, ad un nuovo approccio verso la digitalizzazione della pubblica amministrazione e si estende l'applicazione degli strumenti telematici e delle nuove ICT a molteplici aree del settore pubblico: all'università, alla giustizia, ai trasporti, al commercio, al telelavoro, alle università e alla ricerca. Nascono persino nuove forme di partecipazione diretta e di inclusione del cittadino nelle scelte del processo decisionale democratico: con strumenti come l'e-voting o consultazioni on-line, che ci permettono di parlare più compiutamente di e-Democracy.

Il primo atto ufficiale dell'Europa verso la società dell'informazione globale è riscontrabile nella riunione di Bruxelles del dicembre 1993, quando il Consiglio europeo ha chiesto che una relazione, preparata per la riunione del 24-25 Giugno 1994 a Corfù da un gruppo di specialisti sulle misure specifiche nel settore delle infrastrutture dell'informazione, fosse presa in considerazione dalla Comunità e dagli Stati membri. Sulla base di tale relazione, il Consiglio adotterà successivamente un programma operativo per la definizione di precise procedure di intervento e per l'individuazione dei mezzi necessari alla sua realizzazione. Questo rapporto (denominato Bangemann dal nome del suo relatore) esorta l'Unione europea a porre la sua fiducia nei meccanismi di mercato come forza motrice per andare verso l'*Information Age*. Tra l'altro, qui viene affrontato il problema della disparità tra chi ha accesso alle nuove tecnologie e chi ne è privo, con chiaro riferimento ad uno dei problemi più importanti della società dell'informazione: il *digital divide*.

Vi si legge "La rivoluzione digitale produce profondi cambiamenti nella nostra società (...) Il rischio principale consiste nella creazione di una società a due livelli di possessori e di non-possessori, nella quale solo una parte della popolazione ha accesso alle nuove tecnologie e le padroneggia assicurandosene i benefici."

L'evoluzione storica di questo primo approccio dell'Europa all'idea programmata di Stato virtuale/digitale si osserva attraverso la produzione di atti, di programmi politici e operativi che giungono fino all'attuale Agenda digitale europea.

¹⁸ Ivi.

Con il passaggio al nuovo millennio e all'indomani del clamore suscitato dalle dot-com¹⁹, è stato elaborato un quadro giuridico a livello europeo con l'obiettivo di regolamentare la società dell'informazione e della comunicazione europea e con l'intento di fornire a governi, imprese e cittadini, fondamentali linee guida per orientare il proprio agire. Per esempio, nel maggio 2011, la Commissione europea ha lanciato una consultazione pubblica sul *cloud computing* i cui risultati sono stati presentati in una relazione del dicembre 2011. Anche se è indubbiamente vantaggioso per gli utenti (spesso imprese) soprattutto in termini di scalabilità e di ottimizzazione delle soluzioni, il *cloud computing* comporta infatti alcune sfide di tipo giuridico, in particolare a livello di protezione dei dati (responsabilità in caso di perdita, riservatezza, portabilità...). Le misure proposte in ambito comunitario si sono ben presto rivelate insufficienti a normare un ambito in rapida e continua evoluzione al punto che si è reso necessario adeguare il quadro esistente, trattandolo caso per caso e in modo spesso frammentario. Il legislatore UE ha cercato di affrontare e colmare alcune lacune (ne sono un esempio le recenti disposizioni di legge sull'uso dei cookie sul computer o altri dispositivi) ma, almeno fino a poco tempo, non è stato capace di delineare una politica globale e unitaria. La Commissione europea ha pertanto predisposto un piano d'azione, denominato Agenda Digitale per l'Europa, con l'intenzione di presentare una strategia globale che preveda una modernizzazione del quadro giuridico attualmente esistente affrontando, altresì, questioni di carattere etico, dal momento che il confine tra sfera pubblica e privata sta diventando sempre più labile. Nel dicembre 2012 la Commissione europea ha individuato, dai 101 punti di azione di cui si compone l'Agenda Digitale, sette priorità (o "pilastri") per l'economia digitale e la società, tradotti in altrettanti obiettivi da raggiungere durante gli anni 2013 e 2014.

Lo scopo dell'Agenda Digitale è quello di affrontare nuovi problemi giuridici utilizzando un approccio olistico, che abbracci un campo d'azione più ampio e non si soffermi sulla valutazione puntuale del singolo caso aggiungendo ulteriori tasselli alla costruzione dello Stato digitale (nazionale o sovra-nazionale che sia). Se lo Stato è il suo ordinamento giuridico (Kelsen), allora l'Europa, intervenendo a modificare il quadro giuridico esistente con norme che interessano sempre più spesso e con maggiore efficacia vasti settori dello stato-apparato, ha in programma di diventare essa stessa un Super-Stato digitale.

Questa tendenza si evince dalla lettura dei 7 pilastri dell'Agenda Digitale Europea. Il primo pilastro riguarda l'istituzione di un "Digital Single Market" che prevede, tra l'altro, l'adeguamento della Direttiva sulla privacy e la modifica della Direttiva sul commercio elettronico. Altri elementi di

¹⁹ Il termine Dot-com viene anche utilizzato per identificare quelle aziende che, nate a seguito del notevole surplus di fondi generati dalle venture capital, ed al grande ottimismo del mercato azionario durante la fine del ventesimo secolo, impostarono un business improntato principalmente all'erogazione di servizi via web. Queste aziende, eccessivamente fiduciose nelle potenzialità della rete, si illusero di poter facilmente espandersi, ma si trovarono, in molti casi, a dover fare i conti con la mancanza di idee innovative, di esperienza e di capacità gestionali. Proprio per questo le Dot-com furono le protagoniste, in negativo, della bolla speculativa della New Economy all'inizio degli anni duemila, quando numerose di esse fallirono generando una vera e propria recessione della New Economy. Per questo motivo il termine Dot-com può assumere anche un'accezione fortemente negativa, indicando aziende nate senza un chiaro piano industriale e di marketing, quindi con una mancanza di solidità che facilmente le porta al fallimento. Oltre a queste vi sono ovviamente Dot-com che riuscirono, grazie ad una buona iniziativa imprenditoriale ed alla capacità di offrire servizi più interessanti ed innovativi, a sopravvivere alla bolla speculativa ed a svilupparsi nel corso degli anni. Oggi la maggior parte di queste è acquisita dai grandi operatori del mercato (come ad esempio Google, Microsoft e Yahoo!). <http://it.wikipedia.org/wiki/Dot-com>

attenzione sono la creazione di uno Spazio Europeo Unico di Pagamento, l'ulteriore agevolazione della fatturazione elettronica, la semplificazione di una licenza paneuropea sulle opere *online*, la proposta di una Carta dei diritti *online* nell'UE e la proposta di una piattaforma di risoluzione sulle controversie *online*.

Il secondo pilastro, "Interoperability & Standards", include tecniche e azioni operative per la normalizzazione, la standardizzazione e l'interoperabilità, mentre il terzo "Trust & Security", pone particolare enfasi sulla lotta contro la criminalità e la sicurezza informatica. "Fast and ultra fast Internet access" e "Research and innovation" sono rispettivamente i pilastri quattro e cinque. Le linee di azione del sesto pilastro "Enhancing digital literacy, skills and inclusion" hanno invece lo scopo di affrontare le questioni relative al digitale ponendo l'accento sulla valorizzazione delle competenze. Infine, il pilastro sette, "ICT-enabled benefits for EU society", è destinato a supportare il ruolo delle ITC nella riduzione del consumo energetico, sostenendo la vita dei cittadini più deboli e svantaggiati, rivoluzionando i servizi sanitari e migliorando la fornitura di servizi pubblici. Nella visione dello Stato digitale il quadro giuridico attualmente esistente in Europa ha bisogno di un adeguamento completo al fine di evitare che possa perdere la sua stessa rilevanza in un contesto tecnologico in continua evoluzione. Da tempo la Commissione europea ha come obiettivo quello di aggiornare le norme relative alle ICT rivedendo i diversi strumenti giuridici esistenti e proponendo nuove iniziative in chiave 2.0. Tuttavia è ancora tollerabile il mantenimento di un regime giuridico duale, che disciplini separatamente il mondo offline e quello *online*? È davvero ancora necessario un diritto per l'analogico e uno per il digitale? Considerata la progressiva convergenza tra questi due mondi entro pochi anni potrebbe trovare spazio e applicazione una legislazione 3.0 prodotta e applicata da uno Stato Digitale.

Insomma se una piena e completa digitalizzazione dello Stato ci potrà essere in futuro, questa sarà graduale e indotta attraverso alcune mirate politiche di abolizione degli ostacoli e attraverso la ridefinizione della organizzazione interna delle pubbliche amministrazioni. Accompagnate dalla alfabetizzazione informatica di tutte le categorie dei cittadini.

1. La comunicazione digitale dello Stato moderno

Alcuni diritti, alcune pratiche e diversi concetti di nuovo conio contribuiscono a connotare l'attuale società come prodotta da norme sempre più orientate verso il digitale e che produce a sua volta istanze che inducono gli apparati statali a digitalizzarsi.

Il concetto di *e-democracy* è un prodotto della digitalizzazione dello Stato e della nuova produzione di diritto sollecitata dalle tecnologie della comunicazione. Diversi contributi finora prodotti in tal senso sono intervenuti a caratterizzarne gli ambiti d'influenza sull'amministrazione politica e sulla società, oltre ad analizzare il nuovo modo d'intendere la democrazia, la Pubblica Amministrazione e la società stessa, soffermandosi sulle conseguenze negative dell'arretratezza tecnologica²⁰, anche con un approccio di genere.

L'*e-democracy* potrebbe essere intesa erroneamente come un nuovo tipo di democrazia, estranea al concetto comunemente conosciuto di "potere del popolo", ma in realtà, più che demolire i precetti precedenti, essa ne ristrutturava le fondamenta, dando nuova linfa al concetto di democrazia. Per *e-democracy* s'intende ogni sperimentazione e utilizzo di tecnologie informatiche e telematiche

²⁰ Cfr. P. L. Di Viggiano, R. Bufano, *Donne e società. Partecipazione democratica e cittadinanza digitale*, Tangram, Trento 2013.

al fine di garantire ai cittadini la massima e più agevole partecipazione politica e istituzionale, a qualsiasi livello.

Parlare di *e-democracy* ci porta a parlare anche di *e-government* e dell'impatto che esso ha nello sviluppo dell'apparato democratico mondiale.

L'*e-government*²¹ è posto alla base dell'attuale idea di Stato digitale il quale fonda i suoi mutamenti nello "Stato apparato", risultandone uno strumento essenziale d'evoluzione. La caratteristica principale dell'*e-government* riguarda la possibilità di governo elettronico della cosa pubblica e in particolare la capacità di comunicazione e di gestire le documentazioni della Pubblica Amministrazione con dispositivi telematici digitali i quali, unitariamente a un'azione di cambiamento organizzativo, consentono un'ottimizzazione del lavoro amministrativo e rappresentano un sussidio importante per la costruzione delle decisioni. In presenza di azioni di *e-government* efficaci è garantito l'accesso diretto dei cittadini alle informazioni amministrative, rendendo più efficienti e veloci i servizi e consentendone di nuovi. Uno degli aspetti principali dell'*e-government*, quindi, risiede nell'evoluzione dell'apparato organizzativo della Pubblica Amministrazione, cioè, non solo nell'utilizzo di strumenti di "front office" diretti ai cittadini, ma, soprattutto, nell'introduzione di strumenti di razionalizzazione del "back office" per la gestione interna.

Si intende, quindi, l'*e-government* come strumento essenziale d'evoluzione e di sviluppo dello "Stato apparato", ma l'uragano informatico non si limita a smuovere le fondamenta amministrativo-governative: esso, invero, ha già intaccato in modo irreversibile la società, rendendo disponibili nuove possibilità d'interazione. Alcune suggestioni individuano una nuova *borghesia tecnologica* quale nuova classe emergente all'interno dello Stato digitale l'avvento della quale istituisce, *de facto*, una nuova forma di Stato, ovvero un "terzo Stato digitale", che si va ad affiancare allo "Stato-apparato" e allo "Stato-comunità".

I cittadini dello Stato digitale sono chiamati *Netizen*²², termine con cui s'intende una nuova "borghesia digitale", ovvero i cittadini della Rete, che, al contempo, sono anche cittadini dello "Stato comunità" e possono appartenere allo "Stato-apparato". Non tutti gli utenti del cyberspazio sono identificabili come *Netizen*: sono tali solo coloro che, *online*, contribuiscono attivamente allo sviluppo della Rete. I *Netizen* sono una parte integrante dello "Stato digitale", ma non l'unica. Secondo uno studio del '97 della rivista "Wired", i cybernauti possono esser suddivisi in 4 categorie fondamentali²³:

1. Superconnessi: definiti da Steve Jobs come "digital road warrior", possiedono notebook, desktop, cellulari e cerca persone ed usano molto la posta elettronica;
2. Connessi: usano altrettanto la posta elettronica, ma non posseggono uno dei device sopracitati;
3. Semiconnessi: posseggono uno solo dei device utilizzati dai superconnessi;
4. Non connessi: non possiedono alcuno dei mezzi di comunicazione sopracitati.

Come è facile intuire, vi è una percentuale della popolazione che non fa ancora parte del cosid-

²¹ Cfr. L. Buccoliero, *Introduzione al governo elettronico*, in ID., *Il Governo elettronico. Modelli, strategie di innovazione ed elementi di valore per una pubblica amministrazione digitale*, cit., p. 10 e ss.

²² M. Hauben, R. Hauben, "Netizens: on the history and impact of Usenet and the Internet", IEEE Computer Society Press, Los Alamitos CA 1995, in F. Bollorino, A. Rubini, "Ascesa e caduta del terzo stato digitale. Un promemoria politico per il terzo millennio", cit., p. 84.

²³ Wired, Dicembre 1997, p. 68 e ss. I dati della ricerca realizzata da Wired in associazione con la Merrill Lynch; sono disponibili anche in rete presso il sito Hotwired: <http://www.hotwired.com>.

detto “terzo Stato digitale”: il problema dei “non connessi” continua a essere attuale, visto il maggior grado d’integrazione cibernetica che ci si trova ad affrontare. Tale situazione viene collocata nell’area del *digital divide*, o divario digitale, termine con cui s’intende la discrepanza esistente tra chi ha accesso alle tecnologie informatiche e chi ne è escluso, in modo parziale o totale. Le cause del divario digitale possono essere individuate come dipendenti da diversi fattori, compreso quello economico: nei cosiddetti Paesi in via di sviluppo, invero, ampie fasce di popolazione non sono in grado di accedere alle tecnologie per motivi di reddito. Tuttavia, il fattore economico non rappresenta l’unica causa del *digital divide* il quale si forma come un fenomeno caratterizzato prevalentemente da:

- l’assenza d’infrastrutture (linee telefoniche standard o a banda larga);
- l’analfabetismo informatico, sia riguardo l’uso del computer, sia riguardo le potenzialità di Internet;
- l’appartenenza a determinati gruppi etnici, sociali e culturali;
- le differenze di età e di genere;
- il livello di educazione e il grado di cultura.

Il rischio che gli analisti prevedono è quello secondo il quale, oltre ad incidere in maniera drammatica sul diritto all’informazione, il *digital divide* potrebbe innescare un circolo vizioso tale da portare i Paesi in via di sviluppo ad impoverirsi ulteriormente, in quanto esclusi dalle nuove forme di produzione di ricchezza, basate sui beni immateriali dell’informazione²⁴.

Come abbiamo osservato, sul versante della riflessione d’oltreoceano, secondo la definizione di Jane E. Fountain, lo Stato virtuale è un governo organizzato in modo crescente in termini di amministrazioni virtuali e network pubblico-privati, di cui la struttura amministrativa e le capacità dipendono da Internet e dal web. In altre parole, secondo l’autrice, la Pubblica Amministrazione del futuro dovrà essere del tutto interconnessa, tanto che l’utente finale non potrà più ricondursi alla fonte originaria dell’informazione, grazie alla massiccia integrazione di tutti i settori della Pubblica Amministrazione.

Nello Stato virtuale, i flussi informativi e di comunicazione transitano sul web, piuttosto che attraverso il canale burocratico²⁵. L’*e-government*, quindi, ha come effetto quello di virtualizzare le comunità di riferimento, facendo sostanzialmente scomparire i confini territoriali e superando i limiti geografici²⁶.

Sulla scia di questa suggestione Buccoliero individua tre linee principali della virtualizzazione della Pubblica Amministrazione²⁷:

- i confini della Pubblica Amministrazione iniziano a inglobare le aziende. Ne consegue l’integrazione tra la Pubblica Amministrazione e le aziende che forniscono servizi pubblici;
- i confini della Pubblica Amministrazione si aprono alle penetrazioni, dall’esterno, dei cittadini. Ne consegue la possibilità dei cittadini di accedere a banche dati pubbliche;

²⁴ http://it.wikipedia.org/wiki/Digital_divide; Cfr. S BENTIVEGNA., *Disuguaglianze digitali. Le nuove forme di esclusione nella società dell’informazione*, Laterza, Roma-Bari 2009.

²⁵ Cfr. J. E. Fountain, “*Building the virtual State: Information Technology and Institutional Change*”, cit..

²⁶ L. Buccoliero, *Il Governo elettronico. Modelli, strategie di innovazione ed elementi di valore per una pubblica amministrazione digitale*, cit., p. 11.

²⁷ Cfr. L. Buccoliero, E. Borgonovi, “*L’impatto*”, cit..

-
- i confini della Pubblica Amministrazione si aprono ad altre Pubbliche Amministrazioni, ingrandendosi.
 - Conclusioni

Il percorso attraverso il quale la società contemporanea (che riteniamo ancora non compiutamente moderna in quanto i sistemi sociali che la compongono sono sempre più differenziati, ma non ancora del tutto) si costruisce progressivamente come società dell'informazione e della comunicazione registra una costante tendenza verso la digitalizzazione di ampie aree dello Stato comunque inteso.

Le tecnologie della comunicazione²⁸ producono nuovi assetti per la gestione dello Stato che si orienta sempre più ad essere digitale e i sistemi informativi, unitamente alla reingegnerizzazione delle attività degli apparati burocratici e alle possibilità di accesso e di inclusione dei cittadini pongono i presupposti tecnologici, organizzativi e giuridici di nuove modalità di esercizio della partecipazione.

Anche in Italia possiamo, allora, parlare di nuove forme di esercizio della democrazia²⁹, l'e-Democracy, che si predispose per superare la pratica rappresentativa del consenso e tornare a parlare con piena legittimazione di democrazia diretta resa possibile dalle ICT e dai servizi per l'accesso consentiti dalle tecnologie, dalla politica e dal diritto. Del resto siamo consapevoli dei rischi di abuso che in qualche misura già cominciano a palesarsi, prodotti da un uso strumentale e populista di questo strumento di libertà.

Anche lo stato sociale, o welfare, ormai ha digitalizzato gran parte dei servizi ai cittadini e si parla sempre più di e-Justice attraverso la digitalizzazione delle pratiche di giustizia e l'introduzione nell'ordinamento italiano dei processi telematici. La Sanità, nella sua accezione di e-Health, si serve della telemedicina e garantisce ormai una serie di servizi sanitari e amministrativi fruibili in rete.

La sicurezza informatica è diventato un settore vitale delle politiche degli Stati soprattutto sul versante della difesa della sicurezza e dell'integrità dei dati digitali i quali rappresentano il *core business* e il patrimonio più consistente non solo della PA.

In questo rinnovato scenario, agli albori del III millennio si afferma e si espande, oserei dire con le stesse grandezze di espansione delle reti digitali, un nuovo modo di essere cittadini; si consolidano nuove dimensioni della cittadinanza e nuovi esercizi della stessa. È nata, ormai, la cittadinanza digitale³⁰. Sono nati i cittadini digitali, con un linguaggio digitale e con relazioni sincrone e mobili esercitabili in ogni luogo e in ogni spazio, privato e pubblico.

È l'affermarsi della società della comunicazione. È il trionfo della comunicazione, ormai prevalentemente digitale, interattiva, che travalica gli Stati, tecnicamente regolata dalle norme e dagli apparati statali orientati verso un modello definito di Open government.

La brevità e la incompletezza del presente lavoro non consentono altro se non di avanzare alcune suggestioni, porre delle ipotesi, forse anche delle provocazioni o proiettare visioni utopiche, ma se queste nostre ipotesi hanno una loro plausibilità, se possono essere sostenibili, allora si aprono spazi.

²⁸ Cfr. S. Rodotà, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Laterza, Roma-Bari 2004.

²⁹ Cfr. per un sintetico approccio al tema delle democrazie, D. della Porta, *Democrazie*, Il Mulino, Bologna 2011.

³⁰ Cfr. G. Cogo, *La cittadinanza digitale*, Edizioni della Sera, Roma 2010; Cfr. P.L. Di Viggiano, R. Bufano, *Donne e società*, cit..

Bibliografia

- AA:VV., *Il progetto Cybersyn. Cibernetica per la democrazia*, (A cura di F. De Cindio e G. De Michelis), CLUP-CLUED, Milano 1980.
- Bentham J., *Panopticon ovvero la casa d'ispezione* (a cura di M. Foucault e M. Pierrot), Marsilio, Venezia 1983. [Ed. originale: *Panopticon or the inspection-house*, T. Payne, London 1791].
- Bentivegna S., *Disuguaglianze digitali. Le nuove forme di esclusione nella società dell'informazione*, Laterza, Roma-Bari 2009.
- Bollorin F., Rubini A., *Ascesa e caduta del terzo stato digitale. Un promemoria politico per il terzo millennio*, Apogeo, Milano 1999.
- Buccoliero L., Borgonovi E., *L'impatto delle tecnologie dell'informazione e della comunicazione sulle amministrazioni pubbliche. Principi e sistemi aziendali per le amministrazioni pubbliche*, EGEA, Milano 2000.
- Buccoliero L., *Il Governo elettronico. Modelli, strategie di innovazione ed elementi di valore per una pubblica amministrazione digitale*, Tecniche nuove, Milano 2009.
- Cogo G., *La cittadinanza digitale*, Edizioni della Sera, Roma 2010
- della Porta D., *Democrazie*, il Mulino, Bologna 2011.
- Di Viggiano P. L., Bufano R., *Donne e società. Partecipazione democratica e cittadinanza digitale*, Tangram, Trento 2013
- Fountain J. E., *Building the Virtual State: Information Technology and Institutional Change*, Brookings Institution Press, Washington D.C. 2001.
- Hauben M., Hauben R., *Netizens: on the history and impact of Usenet and the Internet*, IEEE Computer Society Press, Los Alamitos CA 1995.
- Kelsen H., *Teoria generale del diritto e dello Stato*, Etas, Milano 2009.
- Loevinger L., *Jurimetrics. The Next Step Forward*, Minnesota Law Review, 1949.
- Luhmann N., De Giorgi R., *Teoria della società*, Franco Angeli, Milano 1992.
- Mattioni A., Fardella F., *Teoria generale dello Stato e della Costituzione. Un'antologia ragionata*, Giappichelli, Torino 2009.
- Orwell G., *1984*, Arnoldo Mondadori Editore, Milano 2000.
- Rodotà S., *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Laterza, Roma-Bari 2004.
- Saraceno C., *Il Welfare. Modelli e dilemmi della cittadinanza sociale*, il Mulino, Bologna, 2013.
- Shennan J. H., *Le origini dello stato moderno in Europa*, Il Mulino, Bologna 1991.

Sitografia

<http://it.wikipedia.org/wiki/Dot-com>

http://it.wikipedia.org/wiki/Digital_divide

sito Hotwired: <http://www.hotwired.com>

www.leg.unisalento.it

Rivista elettronica di Diritto, Economia, Management: <http://www.clioedu.it/riviste/diritto-economia-management/index.php>

CONSERVARE IL DOCUMENTO INFORMATICO: UNA CHIMERA PER PA, IMPRESE E PROFESSIONISTI?¹

Andrea Lisi

 *Multimedia*



Clicca sull'immagine o fotografa il QRCode
per accedere al Mediabook CLIOedu

Abstract: La natura di ciò che definiamo come “documento” è profondamente cambiata negli ultimi anni con l’avvento e la diffusione delle tecnologie informatiche, imponendo nuovi interrogativi sui metodi di formazione e conservazione dei documenti informatici. Analizziamo le principali conseguenze di questo cambiamento e quali sono strumenti e professionalità deputati alla gestione dei nuovi flussi documentali digitali.

Parole chiave: digitalizzazione, documento informatico, Codice dell’Amministrazione Digitale, firme elettroniche, fatturazione elettronica, Responsabile Conservazione, Responsabile Trattamento

Sommario: 1.L’evoluzione del documento - 2.La funzione delle Firme elettroniche - 3.Formazione del documento informatico - 4.La fatturazione elettronica - 5.Il Responsabile della Conservazione digitale e il Responsabile del Trattamento dati

1. L’evoluzione del documento

Nel corso degli ultimi anni, ci siamo confrontati a ritmi sempre crescenti con l’avvento di nuovi sistemi e tecnologie che hanno totalmente rivoluzionato il nostro modo di pensare, lavorare e agire in una misura che, a detta di molti esperti, non trova eguali in altre fasi della storia dell’umanità. In effetti, non abbiamo avuto il tempo di analizzare e comprendere appieno i fenomeni e le conoscenze appena acquisite senza che di lì a poco qualcosa cambiasse nuovamente. In altre parole, ci siamo trovati in balia di una perpetua e sempre più intensa “*forza di distruzione creatrice*”.

Nell’arco di poco più di un decennio, infatti, dal floppy disk al cd, dalla chiave usb al cloud computing, le nostre certezze tecnologiche sono state via via ribaltate e soppiantate dall’arrivo di nuovi strumenti. Grazie soprattutto a quella rivoluzione radicale che è stata l’avvento del web, inoltre, abbiamo dovuto abituarci a un pensiero sempre più dinamico, a non fossilizzare il nostro modo di vedere e concepire le cose, a essere perennemente predisposti al cambiamento.

Mentre tutto si evolve, il concetto di formazione e conservazione del documento non rimane certo fermo, assecondando il modificarsi della natura stessa dei documenti con cui abbiamo a che fare. Se infatti fino agli anni ’90 si aveva del document management una visione più ristretta e univoca, che sostanzialmente coincideva con la digitalizzazione di immagini e l’archiviazione ottica di documenti nati originariamente su supporti analogici (prevalentemente cartacei o comunque speculari alla carta), negli anni 2000 si è passati al concetto già più complesso di “gestione documentale” e conservazione sostitutiva e, cioè, la sostituzione del documento cartaceo con l’equivalente documento digitale, il cui contenuto viene “cristallizzato” grazie all’utilizzo della firma digitale e della marca temporale². Oggi, invece, ci confrontiamo ormai sempre più spesso con processi nativamente digitali, nei quali il documento coincide di frequente con un flusso di dati originato in modo sempre più multicanale e dove, quindi, dell’immagine della carta non c’è più traccia. Tutto questo ci porta a doverci commisurare ogni giorno con un senso di vertigine dettato dall’odierna assenza della necessità del supporto per produrre e preservare i nostri dati, informazioni e documenti

² Garantendone così la sopravvivenza nel tempo come originale “autenticamente” digitale attraverso un sistema di conservazione a norma.

digitali, magari memorizzati in sistemi cloud.

Intanto, come dicevamo, anche la natura del documento è mutata e continua a farlo, forse tanto velocemente che la nostra stessa capacità di concettualizzazione non riesce a starle appresso.

Se per esempio cerchiamo lumi su un'enciclopedia online, potremo riscontrare che per “documento” si intende ancora, in prima analisi, “qualsiasi mezzo, soprattutto grafico, che provi l'esistenza di un fatto, l'esattezza o la verità di un'asserzione”, e solo qualche accezione più in basso si arriva a contemplare anche il “*file* contenente testo o immagini, creato con un *word processor* o con un programma di impaginazione”³, e qui ci si ferma.

Anche facendo una ricerca per immagini su Google con la parola chiave “documento” la netta maggioranza dei risultati che ci troviamo davanti sono ancora foto o icone di documenti cartacei. Invece, il documento non è più solo ciò che di primo acchito la nostra mente assocerebbe a questo nome, ovvero una “carta bollata”, una lettera, un certificato, qualcosa che comunque possa esprimersi nostalgicamente in una forma cartacea, ma qualcosa di molto più dinamico, strutturato e multicanale, come i flussi di informazioni che vengono scambiati e letti quotidianamente dai sistemi informativi e documentali sia delle PA che delle aziende.

Ormai siamo passati dal concetto di gestione documentale garantita dalla assicurante e tecnologicamente orientata firma digitale al concetto molto più ampio e mutevole (ma web 2.0 oriented) di processo digitale autorizzato da varie possibili tipologie di firma. E infatti si è passati dalla firma digitale alla più evanescente firma elettronica, attraverso i presidi più sicuri dei sistemi (tecnologicamente neutrali) della firma elettronica avanzata, sino a ritornare all'illusione della firma autografa con la firma elettronica grafometrica.

Va da sé che nel gestire queste nuove tipologie di documenti si debbano mettere a punto sistemi multicanale e si debba tenere conto delle caratteristiche peculiari di questi flussi informativi, che, rispetto ai loro omologhi analogici, sono innanzitutto più facilmente modificabili e più difficilmente riconducibili al loro autore, viaggiano su canali tendenzialmente insicuri, sono sottoposti al continuo cambiamento tecnologico e, *dulcis in fundo*, non sono facilmente conservabili nel tempo. In tal senso, sappiamo già che l'art. 1, comma 1°, lett. p) del Codice dell'Amministrazione Digitale (di cui al D.Lgs. n. 82/2005) definisce il documento informatico come la “rappresentazione informatica di atti, fatti, dati giuridicamente rilevanti”.

Tale ampia definizione ricomprende elementi di vario genere: da un referto digitale a un tracciato EDI, dai log file generati da una transazione economica su un sito web a una comunicazione e-mail. Tali documenti però, al contrario di quelli cartacei, sono - come abbiamo già precisato - per loro natura più facilmente soggetti a modifiche e duplicazioni e conseguentemente pongono il problema della loro sopravvivenza nel tempo e della loro validità giuridica.

In merito a tale profilo, ai sensi dell'art. 20, comma 1 bis, del Codice dell'Amministrazione Digitale, il documento informatico soddisfa i requisiti della forma scritta quando garantisce in modo oggettivo qualità, integrità, sicurezza e immodificabilità: in base alle medesime caratteristiche, il documento informatico fornito di firma elettronica “semplice” è liberamente valutabile in giudizio, secondo l'art. 21, comma 1, del citato Codice. Già da una prima analisi delle norme, viene dunque in rilievo l'importanza assunta dalle tecnologie scelte per garantire la validità del documento

³ <http://www.treccani.it/vocabolario/documento/>

informatico e, tra queste, rientra sicuramente la firma elettronica.

Infatti, se nel mondo analogico utilizziamo il documento scritto e sottoscritto per avere una documentazione certa che mantenga traccia delle nostre azioni e possa essere utilizzata ed esibita in caso di contestazione, per ottenere le medesime garanzie nel mondo digitale dobbiamo utilizzare processi e sistemi informatici che possano parimenti presidiare i dati informatici garantendone la paternità e preservandone l'integrità/autenticità nel tempo. In questo modo un dato informatico perde le sue caratteristiche "labilmente" informative⁴ per assumere le più "solide" fattezze della documentazione digitale.

2. La funzione delle Firme elettroniche

Nel nostro ordinamento sono disciplinati diversi tipi di firme elettroniche: queste contribuiscono a determinare il valore giuridico e probatorio dei documenti informatici a cui sono apposte.

I sistemi di firma elettronica, infatti, si differenziano non solo per le diverse tecnologie utilizzate, ma anche per la loro maggiore o minore capacità di assicurare la presenza di tutti gli elementi idonei a garantire sia l'imputabilità giuridica del documento informatico (cioè la sua provenienza da parte del soggetto firmatario), sia l'integrità e l'immodificabilità del documento in tal modo firmato.

A tale scopo abbiamo nel nostro ordinamento quattro tipologie di firma elettronica (previste dall'art. 1 del CAD):

- **FIRMA ELETTRONICA SEMPLICE** (lett. q) - L'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica;
- **FIRMA ELETTRONICA AVANZATA** (lett. q-bis) - Insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati;
- **FIRMA ELETTRONICA QUALIFICATA** (lett. r) - Un particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma;
- **FIRMA DIGITALE** (lett. s) - Un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.

In questo quadro normativo si inseriscono le nuove soluzioni di firma elettronica avanzata (FEA) che, dopo le modifiche introdotte dal D.lgs. n. 235/2010 al Codice dell'Amministrazione Digitale

⁴ Di "informazione volatile" ha parlato in passato la Corte di Cassazione a proposito di pagine web (Cass. Sez. Lavoro Sent. 02912/04).

e l’emanazione del D.P.C.M. 22 febbraio 2013, recante le nuove “Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali”, sono riapparse prepotentemente sul mercato.

Le Regole tecniche sulla FEA, dettate agli artt. 55 e ss. del citato D.P.C.M., stabiliscono ora che la realizzazione di soluzioni di firma elettronica avanzata è libera e non è soggetta ad alcuna autorizzazione preventiva. I soggetti che erogano sistemi di firma elettronica avanzata, quindi, non sono obbligati ad alcuna registrazione e/o accreditamento e questo dimostra la volontà di liberalizzare le tipologie di firma avanzata, non vincolandole all’utilizzo di un certificato qualificato o di un dispositivo sicuro, come invece richiesto per le firme elettroniche qualificate e per quelle digitali, entrambe *species* del genere firma elettronica avanzata. Ciò in quanto le firme elettroniche avanzate hanno un valore limitato al solo contesto in cui vengono utilizzate (tra il sottoscrittore e il soggetto che offre il servizio di firma), rendendo quindi necessario che le loro condizioni di utilizzo siano preventivamente accettate per iscritto dagli utenti. Per questi motivi, il soggetto che realizza la soluzione di firma elettronica avanzata dovrà correttamente informare gli utenti in merito agli esatti termini e condizioni relativi al servizio, compresa ogni eventuale limitazione dell’uso.

Le soluzioni di firma elettronica avanzata, quindi, non sono costituite da un determinato software, né da una determinata tecnologia, ma rappresentano un sistema neutro, sicuro e affidabile, idoneo a garantire la riconducibilità di un documento informatico, reso imm modificabile, al soggetto che l’ha sottoscritto.

A tal fine, ai sensi dell’art. 56 delle menzionate Regole tecniche, tali soluzioni di firma devono assicurare:

- a) l’identificazione del firmatario del documento;
- b) la connessione univoca della firma al firmatario;
- c) il controllo esclusivo da parte del firmatario del sistema di generazione della firma, ivi inclusi i dati biometrici eventualmente utilizzati per la generazione della firma medesima;
- d) la possibilità di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l’apposizione della firma;
- e) la possibilità per il firmatario di ottenere evidenza di quanto sottoscritto;
- f) l’individuazione del soggetto di cui all’articolo 55, comma 2, lettera a);
- g) l’assenza di qualunque elemento nell’oggetto della sottoscrizione atto a modificarne gli atti, fatti o dati nello stesso rappresentati;
- h) la connessione univoca della firma al documento sottoscritto.

Qualora i sistemi di firma elettronica in concreto adottati non dovessero assicurare i requisiti innanzi richiamati - ad eccezione della lett. f) - la firma elettronica generata non potrà soddisfare le caratteristiche previste dagli articoli 20, comma 1 bis, e 21, comma 2, del CAD, ossia qualità, sicurezza, integrità e imm modificabilità, che costituiscono i parametri del giudizio sul valore probatorio del documento informatico e della sua idoneità e soddisfare il requisito della forma scritta.

Inoltre, è di estrema importanza che tutte le fasi del processo siano correttamente registrate e che i relativi log file siano conservati a norma insieme ai documenti e a tutte le altre informazioni relative al processo di firma elettronica. Un idoneo sistema di conservazione, infatti, è in grado di garantire l’integrità dei dati oggetto di archiviazione e consente l’esibizione dei documenti e delle relative informazioni a essi associate (informazioni che, unitamente al documento di riconoscimento, costituiscono la FEA).

3. Formazione del documento informatico

Nel complesso contesto che abbiamo finora descritto, anche lo stesso concetto di “formazione” del documento informatico si è andato modificando e, in base a quanto espresso dall’art. 3 comma 1 della Bozza di Regole tecniche del documento informatico e gestione documentale⁵, esso ora comprende le seguenti azioni principali:

- a) redazione tramite l’utilizzo di appositi strumenti software;
- b) acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico, acquisizione per via telematica o su supporto informatico;
- c) registrazione informatica delle informazioni risultanti da transazioni informatiche o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all’utente;
- d) generazione o raggruppamento anche in via automatica di un insieme di dati, provenienti da una o più basi dati anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica.

Quindi, ormai si passa da una concezione più tradizionale della formazione del documento prodotto attraverso un software di word processor o attraverso un’acquisizione della sua immagine via scanner a una visione più moderna e dinamica di documento, individuabile come una registrazione durevole di flussi informativi giuridicamente rilevanti⁶.

Tale nuova concezione di documento è peraltro già rinvenibile nella nuova disciplina sulla fatturazione elettronica, introdotta dalla Direttiva europea 2010/45/UE e recepita nel nostro ordinamento attraverso la legge 228/2012 che ha modificato il D.P.R. 26 ottobre 1972, n. 633.

4. La fatturazione elettronica

All’art. 21 del citato provvedimento è stata infatti introdotta la riformulata nozione di fattura elettronica, per la quale ora deve intendersi la fattura che è stata emessa e ricevuta in un qualunque formato elettronico (art. 217 della Direttiva 45/2010/UE); inoltre, la stessa disposizione precisa che la fattura, cartacea o elettronica, si ha per emessa all’atto della sua consegna, spedizione, tra-

⁵ Regole tecniche in materia di formazione, trasmissione, conservazione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici, nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41 e 71, comma 1, del Codice dell’amministrazione digitale di cui al decreto legislativo n. 82 del 2005 (acquisibili in formato bozza sul sito istituzionale di AgID alla pagina <http://www.digitpa.gov.it/sites/default/files/Regole%20tecniche%20doc%20inf%20e%20gest%20documentale%2028%2010%202011.pdf>).

⁶ Del resto la locuzione latina *verba volant scripta manent* andrebbe riadattata e rimodellata in base ai nuovi strumenti di comunicazione multicanale di cui dispone oggi la società digitale e con cui deve fare i conti, ripensando allo stesso ruolo di terze parti fidate che possano cooperare con i contraenti/soggetti che manifestano le loro volontà in ambienti digitali riservati, garantendo a tali manifestazioni di volontà espresse in modo diverso (sotto forma essenzialmente di file di log giuridicamente rilevanti) una staticizzazione e una conservazione in forma digitale autentica.

smissione o messa a disposizione del cessionario o committente. In tal senso, sulla scorta dell'attuale definizione, non tutte le fatture telematiche possono rientrare nella definizione di fattura elettronica di cui all'art. 217 della Direttiva: ad esempio, le fatture create in formato elettronico tramite un software di contabilità o un software di elaborazione di testi e successivamente inviate e ricevute in formato cartaceo non possono rientrare nella definizione della Direttiva 2010/45/UE; diversamente, le fatture create in formato cartaceo, poi scannerizzate, sottoscritte con firma elettronica avanzata (basata su un certificato qualificato e creata mediante un dispositivo per la creazione di firma sicura) e inviate e ricevute tramite posta elettronica, possono invece essere considerate fatture elettroniche ai sensi della normativa europea.

Da queste due ipotesi risulta evidente che per distinguere le fatture elettroniche da quelle cartacee non è rilevante il tipo di formato originario, telematico o cartaceo, della fattura, bensì la circostanza che la fattura sia in formato elettronico quando viene emessa (ossia messa a disposizione) e ricevuta. Inoltre, la nuova formulazione del citato art. 21 del D.P.R. 633/1972 prescrive espressamente che il soggetto passivo assicuri in un unico e presidiato processo documentale l'autenticità dell'origine, l'integrità del contenuto e la leggibilità della fattura dal momento della sua emissione fino al termine del suo periodo di conservazione. Al fine di garantire tali requisiti, la norma impone poi di adottare:

- sistemi di controllo di gestione che assicurino un collegamento affidabile tra la fattura e la cessione di beni o la prestazione di servizi a essa riferibili;
- apposizione della firma elettronica qualificata o digitale dell'emittente;
- sistemi EDI (sistemi di Electronic Data Interchange) di trasmissione elettronica dei dati o altre tecnologie in grado di garantire l'autenticità dell'origine e l'integrità dei dati.

La stessa nozione dinamica di documento è stata accolta dal recente Decreto 11 dicembre 2013, n. 141, con cui è stato emanato il "Regolamento recante norme per la dematerializzazione delle quietanze di versamento alla Tesoreria statale", e attraverso il quale si intende completare la dematerializzazione delle quietanze emesse dalle tesorerie statali a fronte dei versamenti effettuati presso le stesse tesorerie. In particolare, l'art. 6 del citato Decreto stabilisce che "nel rispetto degli accordi stabiliti nell'ambito del Sistema Informatizzato dei Pagamenti della Pubblica Amministrazione, nel Protocollo d'intesa sono definite le modalità di firma dei flussi telematici". In tal senso, dunque, il DMEF n. 141/2013 contempla una nozione dinamica del documento informatico, maggiormente in linea anche con l'art. 3 della bozza delle nuove Regole tecniche sul documento informatico dedicato alla sua formazione, il quale prevede espressamente la "*generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più basi dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica*" (lett. d); ossia apriamo sempre più una strada giuridicamente rilevante ai flussi informativi, che quindi andranno opportunamente inseriti in un sistema di digital preservation. Ciò soprattutto alla luce del fatto che il DMEF n. 141/2013 stabilisce che i flussi informatici in oggetto costituiscono la documentazione giustificativa dei versamenti effettuati all'entrata del bilancio statale da parte degli agenti della riscossione e in sede di presentazione dei conti giudiziari e per i quali, dunque, risulta indispensabile predisporre idonei sistemi di conservazione. Per poter, quindi, gestire correttamente queste nuove tipologie di documenti e informazioni rilevanti bisogna adottare specifici modelli e metodologie "a norma", finalizzati a garantire l'attribuibilità, l'integrità, l'autenticità, la sicurezza, la corretta archiviazione e la conservazione nel tempo a questo patrimonio intangibile di dati digitali.

5. Il Responsabile della Conservazione digitale e il Responsabile del Trattamento dati

Sotto un certo punto di vista, si potrebbe affermare che la dinamicità e l'inafferrabilità di queste informazioni digitali siano paragonabili a quelle della parola, della volontà espressa oralmente. Oggi, per comprendere la realtà digitale e le sue dinamiche evolutive (anche dal punto di vista giuridico), è utile probabilmente riflettere sul fatto che per garantire ufficialità e valore giuridico alla volontà orale ci si è serviti per secoli, e tuttora ci si serve, dell'intervento di pubblici ufficiali, quindi, per fare un esempio, di un notaio che, prestato orecchio ai desideri del cliente o dei soggetti che manifestano in sua presenza la loro volontà in forma collegiale, li trasforma in un documento inoppugnabile (cartaceo o digitale che sia); allo stesso modo, per stabilizzare e preservare nel tempo il valore giuridico di questi flussi di informazioni digitali che ormai costituiscono la forma più evoluta e affascinante delle rappresentazioni informatiche di fatti, atti, dati giuridicamente rilevanti, è necessario che ci sia l'intervento di una terza parte fidata: il Responsabile della conservazione digitale o Digital Preservation Officer (D.P.O.).

Il Responsabile della Conservazione digitale dei documenti potrebbe essere definito come "il custode dell'autenticità del documento privo di peso" e sua è la grande responsabilità di dominare in un'organizzazione tutti i flussi di informazioni e documenti che la attraversano - sia che provengano dall'interno che dall'esterno - e gestirli in ogni fase, dalla creazione alla conservazione, garantendo, attraverso avanzate tecniche di conservazione digitale, a tutti i dati che abbiano un rilievo giuridico la certa paternità, la corretta trasmissibilità e gestione, l'adeguata fascicolazione e archiviazione e, non da ultimo, la necessaria sopravvivenza nel tempo.

Un ruolo cruciale quello del Responsabile conservazione, che richiede una preparazione accurata, mirata e multidisciplinare.

Proprio con l'intenzione di sostenere e regolamentare questa figura professionale (e quella altrettanto importante del Responsabile privacy, suo fidato alleato nei processi documentali digitalizzati di qualsiasi organizzazione⁷) è appena stata fondata l'associazione ANORC Professioni, che ha istituito per entrambi i Responsabili un Registro nazionale, in ottemperanza a quanto stabilito dalla Legge del 14 gennaio 2013 n. 4 sulle professioni non organizzate in Ordini o Collegi.

ANORC Professioni garantirà ai Responsabili iscritti un ciclo virtuoso di formazione e aggiornamento, vigilando sul rispetto delle regole deontologiche e di concorrenza, nella convinzione che la formazione sia davvero la carta vincente per godere senza ombre i vantaggi della digitalizzazione, affidando nelle mani giuste i nostri dati e documenti e garantendone così la sicurezza, l'immodificabilità e la permanenza nel tempo.

⁷ La collaborazione con il Responsabile Privacy e nelle PA con il Responsabile del protocollo, dei flussi documentali e degli archivi, oltre che prevista dall'art. 44, comma 1 bis del CAD è inoltre ribadita nelle nuove Regole tecniche ormai sottoscritte dal ministro D'Alia e in attesa di pubblicazione.

RESPONSABILITÀ DEI FORNITORI DI SERVIZI DI VIDEO HOSTING: ESPERIENZE EUROPEE A CONFRONTO

Marilù Capparelli

 *Multimedia*



Clicca sull'immagine o fotografa il QrCode
per accedere al Mediabook CLIOedu

E-PROCUREMENT ED INNOVAZIONE. PIÙ ORGANIZZAZIONE CHE TECNOLOGIA

Michele Melchionda

 *Multimedia*



Clicca sull'immagine o fotografa il QrCode
per accedere al Mediabook CLIOedu

RISORSE UMANE DIGITALI: EVOLUZIONE INFORMATICA E CAPACITÀ DEL PERSONALE PUBBLICO

Giampaolo Teodori

 *Multimedia*



Clicca sull'immagine o fotografa il QrCode
per accedere al Mediabook CLIOedu

IL VALORE ECONOMICO DEL DATO PUBBLICO NELLE SMART CITIES: GLI OPEN DATA PER LO SVILUPPO DEL TERRITORIO

Luca Caputo

 *Multimedia*



Clicca sull'immagine o fotografa il QrCode
per accedere al Mediabook CLIOedu

Contenuto: La vera sfida delle Smart Cities, troppo spesso pensate e progettate esclusivamente come contenitori di tecnologie, è quella di ripensare profondamente se stesse in un mondo in cui il dato pubblico è di fondamentale importanza per favorire la nascita e la crescita di piattaforme di dati e di persone che accedono, utilizzano e creano altra informazione utile a generare nuova conoscenza, nuovo valore e dinamiche innovative. Una città intelligente, sostenuta da politiche di Open Government, è una città che diffonde Open Data e utilizza i dati prodotti e riutilizzati dai city-users per prendere decisioni, per migliorare la qualità della vita, per favorire meccanismi di conoscenza condivisa e generare valore economico, creando opportunità lavorative per i nuovi artigiani digitali.

Abstract: Smart Cities, too often conceived and designed exclusively as containers of technologies, are called to profoundly rethink themselves in a world in which Public Data are important to encourage the creation and growth of platforms and data people accessing, using and create other useful information to generate new knowledge, new value and innovative dynamics. A Smart City, supported by policies of Open Government, is a city that spreads Open Data and uses data produced by city-users to take decisions, to improve quality of life, in order to encourage shared knowledge and generate economic value creating jobopportunities for new digital makers.

Parole chiave: valore, dati pubblici, procedimento, Open Data, Open Government, Smart City, trasparenza, partecipazione, sviluppo, territorio.

Sommario: Introduzione – 1. Il valore economico dei procedimenti – 2. I dati pubblici: trasparenza e partecipazione – 3. Open Data, Smart Cities e sviluppo del territorio – Conclusioni

“Una delle radici della cattiva amministrazione, della burocratizzazione intesa in senso peggiore, consiste proprio nella pretesa di molti cattivi funzionari di limitarsi ad *applicare* le norme: essi, così facendo, esercitano la loro discrezionalità in maniera non consapevole e comunque non orientata alla risoluzione dei problemi - che sono appunto di competenza dell'amministrazione e sono la ragion stessa della sua esistenza - bensì orientata unicamente all'illusorio, mistificante adempimento delle disposizioni ricevute dall'alto.”

(Massimo Corsale, *L'autunno del Leviatano*, 1998)

“I ceppi dell'umanità tormentata sono fatti di carta bollata.”

(Franz Kafka, in Gustav Janouch, *Colloqui con Kafka*, 1951)

Introduzione

Nel 1981, registrare un'automobile a Minneapolis era un continuo accumulo di documentazione e tutto il processo era realizzato di persona. L'ufficio era pieno di lavoro soprattutto all'ora di pranzo e a fine giornata, quando la gente riusciva a ritagliarsi un attimo di tempo per avviare le pratiche. Le attese erano lunghe e i procedimenti farraginosi, spesso c'erano errori nei moduli compilati che

gli impiegati cercavano di correggere mentre altri clienti attendevano sfiniti il loro turno. Dal 2002, fortunatamente, il processo di rinnovamento della registrazione delle autorizzazioni è stato completamente trasformato, consentendo all'utente di scegliere tra tre opzioni: poteva andare allo sportello ed attendere, poteva inviarla per posta all'ufficio o poteva completare l'operazione completamente on line, pagamento compreso.

Finalmente, dopo più di vent'anni, il contribuente poteva avviare una pratica amministrativa quando voleva, nel modo in cui voleva, *dove* voleva. Inoltre, cosa ancora più importante, una profonda analisi delle procedure aveva portato all'identificazione di otto processi di lavoro, ognuno con numerosi sottoprocessi: solo uno di essi, tanto per fare un esempio, richiedeva in media 40 giorni. Quando si esaminò nello specifico l'intero procedimento si scoprì che soltanto 14 ore erano di effettivo lavoro: il resto, infatti, era occupato da passaggi (a volte inutili) da un impiegato all'altro, da un ufficio all'altro, con continue registrazioni e fotocopie sempre degli stessi fascicoli. Nel passare ad un sistema informatizzato si resero conto che, per quanto si volesse riaggiustare il sistema esistente, esso non avrebbe mai consentito il raggiungimento degli obiettivi desiderati semplicemente perché era un sistema basato sulla prassi e, per questo motivo, fu chiesto ai dipendenti di partecipare alla creazione di un nuovo sistema, ripartendo da zero. Solo dopo aver ridisegnato i principali procedimenti il nuovo progetto cominciò a dare i primi risultati: moduli e servizi personalizzati, tempistiche dimezzate, qualità del lavoro migliore per i dipendenti.

1. Il valore economico dei procedimenti

Ogni procedimento avviato in una Pubblica Amministrazione, dunque, ha un valore economico che – se inserito in un sistema virtuoso – aumenta la qualità e la quantità dei servizi offerti, gratifica il lavoro del personale interno e favorisce il trattamento dei dati nell'ottica della trasparenza e di quella che sta diventando, a tutti gli effetti, l'economia degli Open Data.

I dati pubblici diventano una risorsa per la PA che li produce e per l'utenza che ne fruisce, prova ne sia la direttiva *Open Government* (2009) del governo statunitense con cui si stabilisce che i dati, alla stregua di altre risorse, rappresentano materia prima per la produzione di beni e servizi. Per la prima volta, dunque, si attribuisce un valore economico di fondamentale importanza ai dati pubblici e, di riflesso, alle procedure che ne determinano la creazione, la gestione e la condivisione all'interno e all'esterno dell'organizzazione.

In Italia, purtroppo, nonostante l'utilizzo delle nuove tecnologie dell'informazione e della comunicazione (ICT), la PA opera in un regime burocratico in cui la prassi diventa essa stessa il criterio con cui oliare i meccanismi della macchina amministrativa¹. In altre parole, l'esistenza di una procedura è garanzia sufficiente perché non si dubiti della sua immutabilità o, peggio ancora, della sua inevitabilità: *si fa così perché si è sempre fatto così*.

D'altra parte, nonostante la modernizzazione hardware e software delle strutture pubbliche, le tecnologie (aggiuntive e non sostitutive) non hanno ridotto né permesso di eliminare le vecchie pratiche (stampe, fotocopie, timbri, registri di passaggio). Invece di preoccuparsi di ridisegnare

¹ Cfr. P. Ravaioli, *La gestione delle risorse umane negli Enti Locali*, Milano, FrancoAngeli, 2001

i processi chiave, eliminando fasi e passaggi inutili, si è pensato di automatizzare procedimenti burocratici comunque inefficienti, costosi e capaci di generare ritardi, errori e perdite di informazioni.

Nell'Economia della conoscenza, nella Società dell'informazione, nell'era della Smart City il vero spreco di risorse è la perdita di dati: vincono le amministrazioni che sanno condividere conoscenza. Prima ancora di un problema tecnologico, dunque, per la PA si pone un vero e proprio problema di organizzazione interna, mirata a razionalizzare e semplificare non solo le procedure ma anche la vita dei cittadini.

La realizzazione di una città (o un territorio) intelligente passa attraverso una sempre più crescente convergenza verso approcci che puntino a integrare i back-office, senza trascurare la necessità di adottare scelte organizzative che abbattano la frammentazione dei processi e delle responsabilità all'interno delle amministrazioni.

Occorre passare da una cultura dell'adempimento (rispetto regole e procedure) a una cultura del risultato (efficacia, efficienza, economicità), iniziando a innovare utilizzando le tecnologie per sviluppare processi di riorganizzazione che vedono l'utenza (cittadini, imprese, turisti) al centro di tutto e il dato come elemento da valorizzare, conservandone l'integrità e mettendolo a disposizione come se fosse a tutti gli effetti un bene di prima necessità.

I processi vanno personalizzati per venire incontro alle esigenze del *city-user*² e per sradicare quei dogmi culturali che ostacolano il processo di modernizzazione. L'idea di personalizzare i servizi, di migliorare la qualità dell'azione amministrativa, di puntare alla soddisfazione dell'utenza rimette in discussione il fatto che i dipendenti della PA non debbano esclusivamente seguire regole e procedure (prassi) ma prendere decisioni per conto proprio. Se il servizio all'utenza è la priorità, se la produzione di dati è un obiettivo fondamentale allora chi opera nell'amministrazione deve avere la discrezionalità di decidere cosa fare per migliorare i procedimenti³. Non è più la norma il criterio con cui innovare – basti pensare che in Italia si erogano ancora norme per vietare l'uso dei fax nelle comunicazioni con la PA – ma la convenienza (economica, sociale, organizzativa): *si è sempre fatto così ma costa meno e offro un servizio migliore iniziando a farla diversamente*.

2. I dati pubblici: trasparenza e partecipazione

La Pubblica Amministrazione, al pari di una qualsiasi organizzazione complessa, produce, tratta e scambia una grande quantità di dati che servono per garantire l'operatività e l'erogazione dei servizi al cittadino. Grazie allo sviluppo dell'Information & Communication Technology e all'applicazione di meccanismi di eGovernment, tali dati sono ormai messi a disposizione in formato digitale e possono quindi essere condivisi e diffusi. Per fare ciò, tuttavia, è fondamentale identificarne l'origine nell'ambito della struttura burocratica dell'Ente.

² Cfr. M. Vianello, *Smart Cities: Gestire la complessità urbana nell'era di Internet*, Santarcangelo di Romagna, Maggioli Editore, 2012

³ Cfr. M. Mancarella (a cura di), *La Pubblica Amministrazione tra management, eGovernment e federalismo*, Trento, Tangram, 2011

Decidere quali sono i dati di interesse per la Comunità detenuti dalla propria Amministrazione richiede quindi – come primo passaggio – una vera e propria mappatura dei dati complessivamente disponibili.

I dati pubblici a disposizione variano dai dati geografici a quelli demografici, da quelli tributari a quelli legati alla pianificazione urbanistica, fino ad arrivare a quelli che – anche se in formato grezzo – rappresentano un potenziale economico per i professionisti che vogliono utilizzarli ai fini dello sviluppo di nuovi servizi per la comunità.

Mettere a disposizione del cittadino e delle imprese l'insieme dei dati pubblici gestiti dall'Amministrazione in formato aperto rappresenta un passaggio culturale necessario per il rinnovamento delle istituzioni nella direzione di apertura e trasparenza proprie dell'Open Government, a tutti i livelli amministrativi.

Il libero accesso all'informazione pubblica si configura infatti come un aspetto fondamentale per tradurre il concetto di Open Government in un vero e proprio modello sostenibile, in quanto consente di rendere l'amministrazione aperta e trasparente.

Il libero accesso a documenti, atti e saperi sul governo pubblico e sulle scelte politico-istituzionali compiute dalle Amministrazioni è un aspetto centrale per la trasparenza delle Istituzioni. Tale aspetto stimola e facilita i cittadini ad un controllo continuo e costante sull'operato e sui processi decisionali dei soggetti istituzionali, attivando meccanismi virtuosi di controllo collettivo.

Attraverso l'attuazione di politiche di apertura reale delle informazioni e dei dati pubblici, i cittadini sono in condizione di verificare l'efficienza dell'apparato burocratico, aumentando anche la fiducia riposta nell'amministrazione⁴. Distribuire i dati pubblici in un formato aperto e libero da restrizioni sia dal punto di vista dell'accesso che dell'integrazione e del riutilizzo, rappresenta il presupposto di base affinché possa svilupparsi un vero e proprio processo di collaborazione tra le istituzioni e la comunità dei cittadini sulle scelte di governo, anche la rielaborazione in forma nuova e diversa dei dati messi a disposizione. In questo senso, sono esemplari i casi di Canada e California.

In Canada, a partire dalla richiesta di un comune cittadino, si avvia un'analisi nel settore della beneficenza, un giro d'affari quantificato in più di tre miliardi di dollari. Si scopre che "United Way of Greater Toronto" - l'Ente più conosciuto di raccolte benefiche – registra donazioni per un ammontare di 107,5 mln \$ (2008) e risulta essere non prima ma terza nella speciale classifica di settore. Inoltre, sempre grazie a questa ricerca, si evidenzia come quattro delle top 15 associazioni di carità non fossero conosciute dagli addetti del settore. Analisi più approfondite portano alla scoperta di un giro di donazioni fraudolente che utilizzavano questi Enti sommersi per un volume di evasione fiscale pari a 1 mld \$ all'anno, che rappresentava circa il 6% del budget Governo Federale.

In California, invece, le autorità hanno disposto la realizzazione di un sito in cui i visitatori (cittadini, imprenditori, turisti) segnalano e riportano le spese, le procedure, i moduli ritenuti non necessari. Questa collaborazione tra utenza e PA, a fronte di un costo di 21.000 \$ per implementare il sito e di costi per la gestione sotto i 50.000 \$ annui, ha consentito finora allo Stato un risparmio di 20.000.000 \$ sul bilancio pubblico, senza dimenticare il miglioramento e la qualità dei servizi resi

⁴ Cfr. C. Rogate – T. Tarquini, *Fiducia e responsabilità nel governo dell'ente pubblico*, Santarcangelo di Romagna, Maggioli, 2008

alla comunità. Naturalmente non è un caso che le buone prassi vengano da oltreoceano, visto che gli USA investono nella trasparenza e nella cultura degli Open Data: la legge americana sul diritto all'informazione ha un costo di circa 416 milioni di dollari, cioè meno di 1,4 dollari per ogni cittadino. In Italia, secondo gli ultimi dati della Corte dei Conti, il costo della corruzione e della poca trasparenza amministrativa è di oltre 60 miliardi di euro, vale a dire circa 1000 euro per ogni cittadino, in aggiunta alle ricadute economiche, sociali e politiche che una siffatta situazione comporta.

Le buone prassi esposte, dunque, dimostrano come - attraverso strategie di apertura dei dati della Pubblica Amministrazione - i cittadini non sono più soltanto consumatori passivi di informazioni messe a disposizione dalle Amministrazioni. Hanno invece l'opportunità di riutilizzare e integrare i dati messi loro a disposizione, fino a sviluppare servizi e applicazioni a vantaggio dell'intera comunità di utenti, che vanno ad affiancarsi a quelli creati centralmente dalle Istituzioni. In questo modo i cittadini collaborano effettivamente con i soggetti istituzionali e partecipano attivamente alle azioni di governo della cosa pubblica⁵.

Il complesso dei provvedimenti, anche normativi, detta alcuni principi fondamentali che obbligano la PA ad essere trasparente in modo nuovo. Nell'ordinamento giuridico italiano, la trasparenza, e più in generale la disciplina del rapporto dialogico tra Pubblica Amministrazione e cittadino, è un istituto di recente introduzione, essendo stata prevista solo dalla Legge n. 241/1990. Da quel momento, essa è diventata corollario del principio di buona amministrazione costituzionalmente garantito dall'art. 97 Costituzione: infatti, è previsto che "l'attività amministrativa (...) è retta da criteri di economicità, di efficacia, di imparzialità, di pubblicità e di trasparenza" (art. 1, Legge n. 241/1990).

Tuttavia, si tratta di un principio tutt'altro che statico: la trasparenza, infatti, costituisce uno dei gangli del diritto pubblico maggiormente soggetto all'evoluzione politica, sociale e tecnologica⁶. Ed infatti, dopo l'introduzione dell'informatica nell'attività amministrativa e il ripensamento sul ruolo del settore pubblico, l'originario concetto di trasparenza - circoscritto al diritto di accesso agli atti e ai documenti per coloro che avessero specifico e concreto interesse - ha iniziato a dimostrarsi insufficiente.

La digitalizzazione dell'attività amministrativa conferisce nuovi significati al concetto di trasparenza. In proposito, è opportuno ricordare come il Codice dell'Amministrazione Digitale (D. Lgs. n. 82/2005), prevede che "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" (art. 12, D. Lgs. n. 82/2005). Questo significa che le Amministrazioni sono tenute per legge ad assicurare "la disponibilità, la gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione in modalità digitale" (art. 2, D. Lgs. n. 82/2005). A tal fine è inoltre previsto che "i dati delle pubbliche amministrazioni sono formati, raccolti, conservati, resi disponibili e accessibili con l'uso delle tecnologie dell'informazione e della comunicazione che ne consentano la fruizione e riutilizzazione da parte delle altre pubbliche amministrazioni e dai privati" (art. 50, D. Lgs. n. 82/2005).

⁵ Cfr. L. Caputo (a cura di), *Politiche dell'ambiente e del territorio*, Trento, Tangram Edizioni Scientifiche, 2011

⁶ Cfr. D.A. Limone, *Elementi di Diritto dell'Informatica*, Lecce, Adriatica Editrice, 1999

In tale mutato contesto normativo, il Legislatore è successivamente intervenuto, nel 2009, ponendo una nuova concezione normativa di trasparenza, intesa come “accessibilità totale (...) delle informazioni concernenti ogni aspetto dell’organizzazione, degli indicatori relativi agli andamenti gestionali e all’utilizzo delle risorse per il perseguimento delle funzioni istituzionali, dei risultati dell’attività di misurazione e valutazione”, così introducendo nel nostro ordinamento una nuova posizione qualificata in capo a ciascun cittadino, rispetto all’azione degli Enti, con il preciso “scopo di favorire forme diffuse di controllo del rispetto dei principi di buon andamento e imparzialità” (art. 11, D. Lgs. n. 150/2009).

Detta in sintesi, alla luce di quanto esposto, il concetto di trasparenza ha vissuto un’evoluzione sostanziale: non può essere più soltanto uno strumento finalizzato al controllo del procedimento amministrativo, bensì un vero e proprio risultato dell’azione amministrativa; non più, dunque, solo un criterio informatore, ma un obiettivo.

3. Open Data, Smart Cities e sviluppo del territorio

Si può quindi affermare che non c’è vera trasparenza se l’Amministrazione non rende pubbliche on line le informazioni formate e raccolte nell’esercizio della propria attività: tale concetto si ricava, in maniera assai significativa, dalla Delibera n. 105/2010 della Commissione per la Valutazione la Trasparenza e l’Integrità delle Amministrazioni Pubbliche.

Nella definizione di una strategia di Open Data è bene identificare priorità relative all’apertura di dati che siano funzionali ai reali interessi della Comunità di riferimento. In tal senso, la stessa definizione delle priorità può diventare un’occasione di confronto con il cittadino e la comunità locale, che può essere interpellata e coinvolta nella definizione dei dati da aprire.

Tuttavia, nel momento in cui si avvia una strategia di apertura dati non è necessario identificare immediatamente tutti gli usi che verranno fatti di un dato. Spesso è la comunità degli utenti a identificare nei dati un valore che l’Amministrazione stessa non vi ha visto o non vi si ravvede. In linea generale, quindi, quando un dato è disponibile senza che la sua estrazione rappresenti un costo significativo, è opportuno provvedere alla sua apertura anche nel momento in cui non se ne ravveda un’utilità immediata. Spesso, infatti, indicatori di interesse per la Comunità sono desumibili da elaborazioni su dati di base che non erano state previste da chi tale dato ha provveduto ad aprirlo. È bene sottolineare ancora una volta come la logica dell’Open Data spinga comunque l’Amministrazione verso la distribuzione dei dati, anche nel caso in cui questi non fossero disponibili in un formato aperto. In altri termini, se un dato ritenuto utile non è disponibile in un formato strutturato o non si ha la possibilità di convertirlo facilmente in un formato aperto, è comunque meglio distribuirlo anche in forma grezza piuttosto che non distribuirlo affatto. Anche in questo caso, sarà poi la comunità di sviluppatori ad occuparsi della conversione del dato in un formato aperto, e quindi utilizzabile.

Partendo dal concetto di conoscenza aperta così come delineato dalla Open Knowledge Foundation⁷, anche l’Open Data può essere caratterizzato dai seguenti principi:

⁷ www.okfn.org

-
- disponibilità e accesso: i dati devono essere disponibili nel loro complesso, per un prezzo non superiore a un ragionevole costo di riproduzione, preferibilmente mediante scaricamento da Internet. I dati devono essere inoltre disponibili in un formato utile e modificabile;
 - riutilizzo e redistribuzione: i dati devono essere forniti a condizioni tali da permetterne il riutilizzo e la redistribuzione. Ciò comprende la possibilità di combinarli con altre basi di dati;
 - partecipazione universale: tutti devono essere in grado di usare, riutilizzare e redistribuire i dati. Non devono essere poste discriminazioni di ambiti di iniziativa in riferimento a soggetti o gruppi. Per esempio, il divieto di utilizzare i dati per scopi commerciali o le restrizioni che permettono l'uso solo per determinati fini (quale quello educativo) non sono contemplabili.

Per garantire i principi sopra elencati è necessario che i dati, per considerarsi aperti in base agli standard internazionali, siano:

- Completati. I dati devono comprendere tutte le componenti (metadati) che consentano di esportarli, utilizzarli on line e off line, integrarli e aggregarli con altre risorse e diffonderli in rete;
- Primari. Le risorse digitali devono essere strutturate in modo tale che i dati siano presentati in maniera sufficientemente granulare, così che possano essere utilizzate dagli utenti per integrarle e aggregarle con altri dati e contenuti in formato digitale;
- Tempestivi. Gli utenti devono essere messi in condizione di accedere e utilizzare i dati presenti in rete in modo rapido e immediato, massimizzando il valore e l'utilità derivanti da accesso e uso di queste risorse;
- Accessibili. I dati devono essere resi disponibili al maggior numero possibile di utenti senza barriere all'utilizzo, quindi preferibilmente attraverso il solo protocollo Hypertext Transfer Protocol (HTTP) e senza il ricorso a piattaforme proprietarie. Devono essere inoltre resi disponibili senza alcuna sottoscrizione di contratto, pagamento, registrazione o richiesta;
- Leggibili da computer. Per garantire agli utenti la piena libertà di accesso e soprattutto di utilizzo e integrazione dei contenuti digitali, è necessario che i dati siano machine-readable, ovvero processabili in automatico dal computer;
- In formati non proprietari. I dati devono essere codificati in formati aperti e pubblici, sui quali non vi siano entità (aziende o organizzazioni) che ne abbiano il controllo esclusivo. Sono preferibili i formati con le codifiche più semplici e maggiormente supportati;
- Liberi da licenze che ne limitino l'uso. I dati aperti devono essere caratterizzati da licenze che non ne limitino l'uso, la diffusione o la redistribuzione;
- Riutilizzabili. Affinché i dati siano effettivamente aperti, gli utenti devono essere messi in condizione di riutilizzarli e integrarli, fino a creare nuove risorse, applicazioni e servizi di pubblica utilità;
- Ricercabili. I dati devono essere facilmente identificabili in rete, grazie a cataloghi e archivi facilmente indicizzabili dai motori di ricerca;
- Permanenti. Le peculiarità fino ad ora descritte devono caratterizzare i dati nel corso del loro intero ciclo di vita.

Nell'epoca della condivisione dei dati ciò che attribuisce un valore al territorio, più che la dimensione territoriale in sé, è la dimensione delle reti e la qualità delle interazioni che si sviluppano nel collegare le attività umane.

Le politiche di Open Government, incentivate dalla messa a disposizione dei dati in formato open e dalla partecipazione dell'utenza, devono mirare a creare i presupposti per la nascita di Smart Cities sempre più connesse e *produttrici* di conoscenza.

Una Smart City non può essere semplicemente l'insieme delle tecnologie disseminate sul territorio: è un nuovo modo di concepire l'amministrazione⁸, è il modo in cui le persone vengono messe nelle condizioni di usare la tecnologia, anche e soprattutto per sviluppare nuova conoscenza e nuove opportunità lavorative. Questo è ciò che rende intelligente una città, poiché essa diventa il luogo dove si utilizzano in modo sistematico ed organizzato i dati e la conoscenza generati dall'uso delle ICT. È quell'area urbana dove le persone hanno a disposizione *conoscenza virtualizzata* in modo diffuso grazie alla possibilità di connettersi ad Internet.

Nel novembre del 2010 è stato presentato il “Manifesto per l'Open Government” che elenca gli 11 modi per fare Open Government:

1. Governare con le persone.
2. Governare con la rete.
3. Creare un nuovo modello di trasparenza.
4. Trattare l'informazione come infrastruttura.
5. Liberare i dati pubblici per lo sviluppo economico del terzo millennio.
6. Informare, coinvolgere, partecipare per valorizzare l'intelligenza collettiva⁹.
7. La rete moltiplica il potenziale delle intelligenze coinvolte e aumenta l'efficacia dell'azione amministrativa.
8. Educare alla partecipazione.
9. Promuovere l'accesso alla Rete.
10. Costruire la fiducia e aumentare la credibilità della pubblica amministrazione.
11. Promuovere l'innovazione permanente nella Pubblica Amministrazione.

Una serie di dati (c.d. *dataset*) governativi sono stati aperti negli ultimi anni in tutto il mondo. Il primo e più importante, come già accennato in precedenza, è stato *data.gov* americano, lanciato dal governo Obama a seguito della Direttiva sull'Open government nel dicembre 2009 come misura anti-crisi, per permettere di produrre beni e servizi attraverso i dati aperti intesi come materia prima. Anche in Spagna, dove negli ultimi anni notevoli sono stati gli sforzi di attuare politiche di Open Government, le politiche di Open Data hanno portato alla realizzazione di Smart Cities che funzionano come un vero e proprio laboratorio digitale per le nuove competenze richieste dai settori trainanti l'economia: nuove professionalità nei servizi al turismo digitale, nuovi servizi attivati nel campo della domotica e della sanità digitale, nuove professionalità legate alla Pubblica Amministrazione. I nuovi posti di lavoro legati a queste politiche hanno alimentato nel primo anno un giro d'affari di 600 mln di euro legato al Public Sector Information (PSI). È la conferma che i dati che le PA producono, raccolgono, organizzano e utilizzano nello svolgimento dei loro compiti istituzionali hanno un valore intrinseco che va oltre l'assolvimento dei compiti istituzionali dell'ente che le detiene/gestisce.

⁸ Cfr. P.L. Di Viggiano, *L'amministrazione digitale negli Enti Locali. I modelli organizzativi e gli strumenti tecnico-giuridici*, in Il Codice dell'Amministrazione Digitale e forme negoziali telematiche, a cura di Marco Mancarella, Editrice UNI Service, Trento, 2009

⁹ Cfr. G. Preite (a cura di), *Politica e tecnologie*, Roma, Carocci, 2010

Conclusioni

L'informazione detenuta dal settore pubblico rappresenta dunque un patrimonio immenso in ogni ambito – dalla cartografia, alla normativa, alla statistica – fatto di informazioni, dati e contenuti nuovi.

La vera sfida per una Smart City (e di conseguenza per una politica fondata sugli Open Data) è creare e ricreare continuamente le condizioni affinché la condivisione e la conoscenza dei dati portino ad una gestione trasparente e partecipata della macchina amministrativa, a scelte consapevoli e condivise dai cittadini, a servizi di qualità e risparmi sulla spesa pubblica.

Attuare politiche di Open Government consente all'amministrazione di conoscere dati utili al proprio funzionamento e far conoscere dati utili alla propria utenza: determinare il livello di tassazione, informare i cittadini sul modo in cui queste tasse vengono spese, quali servizi attivare, pianificare l'edilizia condividendo i dati in formato aperto con i professionisti del settore e così via. Allo stesso tempo, una cultura degli Open Data deve poter essere la nuova via dell'oro da percorrere per i nuovi artigiani digitali, per lo sviluppo di nuove opportunità lavorative. Non è un caso se Barack Obama, intervenendo in un'assemblea di inaugurazione dell'anno scolastico americano, abbia esortato gli studenti a sfruttare le potenzialità dell'economia digitale: “Non comprate un nuovo videogame: fatene uno. Non scaricate l'ultima app: createla. Non usate semplicemente il vostro telefono: programmatelo.”

Bibliografia

- Caputo L. (a cura di), *Politiche dell'ambiente e del territorio*, Trento, Tangram Edizioni Scientifiche, 2011
- Di Viggiano L., *L'amministrazione digitale negli Enti Locali. I modelli organizzativi e gli strumenti tecnico-giuridici*, in *Il Codice dell'Amministrazione Digitale e forme negoziali telematiche*, a cura di Marco Mancarella, Editrice UNI Service, Trento, 2009
- Limone D.A., *Elementi di Diritto dell'Informatica*, Lecce, Adriatica Editrice, 1999
- Mancarella M. (a cura di), *La Pubblica Amministrazione tra management, eGovernment e federalismo*, Trento, Tangram, 2011
- Preite G. (a cura di), *Politica e tecnologie*, Roma, Carocci, 2010
- Ravaioli P., *La gestione delle risorse umane negli Enti Locali*, Milano, FrancoAngeli, 2001
- Rogate C. – Tarquini T., *Fiducia e responsabilità nel governo dell'ente pubblico*, Santarcangelo di Romagna, Maggioli, 2008
- Vianello M., *Smart Cities: Gestire la complessità urbana nell'era di Internet*, Santarcangelo di Romagna, Maggioli Editore, 2012

IL NUOVO PROGRAMMA HORIZON 2020

Antonio Maria D'Amico

 *Multimedia*



Clicca sull'immagine o fotografa il QrCode
per accedere al Mediabook CLIOedu

BIG DATA E DIRITTO

Sebastiano Faro

 *Multimedia*



Clicca sull'immagine o fotografa il QrCode
per accedere al Mediabook CLIOedu

L'OPEN ACCESS NELLA PIÙ RECENTE NORMATIVA STATALE: UN PASSO AVANTI E DUE INDIETRO¹

Marina Pietrangelo

 *Multimedia*



Clicca sull'immagine o fotografa il QrCode
per accedere al Mediabook CLIOedu

¹ Si pubblica qui, rivista e con corredo di note, la relazione al Convegno dell'Associazione Nazionale Docenti di Informatica Giuridica e Diritto dell'Informatica (ANDIG) "I nuovi scenari della società dell'informazione: aspetti politici, giuridici, amministrativi e tecnici", Roma, 29 ottobre 2013, Università telematica Unitelma Sapienza.

Sommario: 1. Premessa - 1.1. Pro memoria sull'Open Access – 2. L'Open Access nella più recente normativa statale – 3. Per concludere. Dalle resistenze giuridiche alle possibili vie di fuga

1. Premessa

In questa breve riflessione vorrei provare ad indagare le ragioni della resistenza del nostro ordinamento giuridico dinanzi al modello Open Access, utilizzato per la pubblicazione di scritti di carattere scientifico, al quale ancora non sono riconosciuti effetti giuridici pari a quelli assegnati alle tradizionali pubblicazioni scientifiche a stampa. Notoriamente, infatti, solo quest'ultime sono ammesse nelle procedure pubbliche di valutazione dei risultati della ricerca scientifica.²

L'Open Access è stato ampiamente indagato. Le riflessioni, tuttavia, riguardano per lo più le caratteristiche degli archivi e le tecniche dell'archiviazione dal punto di vista biblioteconomico; gli standard tecnici relativi alla costruzione degli archivi stessi dal punto di vista informatico; ma anche, secondo una prospettiva sociologica, i vantaggi per i ricercatori, che attraverso questo tipo di pubblicazione possono più e meglio condividere i propri studi all'interno della comunità scientifica, perchè pubblicati in archivi accessibili a chiunque e dunque più adatti in astratto - rispetto all'editoria tradizionale - a rendere conosciuti i risultati delle ricerche.

Tempo fa mi era parso - ma in fondo mi pare ancora oggi - che mancasse una riflessione del giurista sull'Open Access mirata alla individuazione dei limiti tuttora presenti nel nostro quadro regolatorio, a dispetto delle molte convinte dichiarazioni di favore per il nuovo modello registrabili a livello istituzionale. Dichiarazioni di favore che dovrebbero oramai tradursi in riconoscimenti normativi espressi, che valgano a sottrarre l'Open Access alla occasionalità delle prassi, pure positive, avviate dalle singole istituzioni che operano nel settore della ricerca (almeno di quelle pubbliche); rendendo semmai tali buone pratiche obbligatorie *ex lege*.³

Ancora oggi, se un ricercatore desidera pubblicare un proprio lavoro nel repository Open Access dell'ateneo o dell'ente di ricerca presso cui svolge la propria attività, non ha garanzie che quello scritto (con quei requisiti di forma) sarà ammesso nelle procedure pubbliche di valutazione della ricerca; o nei pubblici concorsi per la progressione nella carriera accademica; o nei concorsi per l'accesso alle scuole di specializzazione etc.

In assenza di norme vincolanti, in grado di garantire uniformemente a livello nazionale un'equiparazione di tali lavori a quelli pubblicati secondo il modello tradizionale, le buone prassi delle singole autonomie universitarie hanno in parte sopperito. Poiché atenei ed enti pubblici di ricerca hanno provveduto alla costruzione di appositi repository, destinati per l'appunto alla raccolta dei lavori scientifici in Open Access prodotti dai propri ricercatori. Ma nella gran parte dei casi si tratta di archivi nei quali sono ripubblicate opere già edite secondo lo schema tradizionale riconosciuto a livello normativo. Resta, dunque, il vero nodo, e cioè - come più volte ricordato - la permanente

² Volendo, v. M. Pietrangelo, *Il valore giuridico delle pubblicazioni scientifiche on-line*, in *Informatica e diritto*, 2, 2009, 171 ss.

³ Sul diritto d'autore e sulle diverse declinazioni dello stesso, particolarmente riguardo alla scelta del singolo autore di pubblicare in Open Access, molto - e bene - è stato scritto. Questi profili non costituiranno, dunque, oggetto della mia riflessione.

assenza di una equiparazione di tali pubblicazioni alle pubblicazioni scientifiche “tradizionali” nell’ambito delle procedure pubbliche di valutazione della ricerca. Nodo che, in definitiva, non spetta sciogliere alle singole autonomie universitarie, ma al legislatore; e che pure le autonomie universitarie potrebbero superare, *in parte qua*, attraverso previsioni espresse - nei propri statuti, regolamenti e bandi di concorso – che consentano di ammettere alla valutazione tali scritti.⁴ Assecondando in tal modo anche l’invito della Commissione europea che da ultimo raccomanda, tra l’altro, che “il sistema delle carriere universitarie *sostenga e premi* [corsivo mio] i ricercatori che aderiscono a una cultura di condivisione dei risultati delle proprie attività di ricerca, in particolare assicurando l’accesso aperto alle loro pubblicazioni nonché sviluppando, incoraggiando e utilizzando nuovi modelli alternativi di valutazione delle carriere, nuovi criteri di misurazione e nuovi indicatori”⁵.

Obiettivo di questa breve riflessione è, dunque, la verifica dello stato dell’arte della normativa nella speciale materia considerata; normativa che, a prima lettura, proprio di recente sembra aver compiuto un passo avanti... e due indietro.⁶

1.1. Promemoria sull’Open Access

Ma cosa deve intendersi per Open Access? Quale è esattamente la forma di pubblicazione che si pone come alternativa alle tradizionali pubblicazioni a stampa curate da un editore privato? La domanda è preliminare alle riflessioni successive, giacché il nostro ordinamento qualifica come pubblicazioni scientifiche solo ed esclusivamente i lavori che presentino - nella forma, evidentemente, cioè nella modalità di disseminazione - certe caratteristiche. E, come di seguito si vedrà, è a quelle regole che occorre guardare, se si è convinti della bontà di questo diverso metodo di pubblicazione, per proporre modifiche ed integrazioni al quadro normativo vigente.

Il movimento dell’Open Access esprime senz’altro, da tempo, un movimento di rottura culturale; con tesi condivisibili in linea di principio, oltre che efficaci dal punto di vista pratico per il ricercatore che abbia a cuore la diffusione dei propri lavori scientifici e la condivisione degli stessi nell’ambito della comunità scientifica.

Dalla nota dichiarazione di Berlino ad oggi non sono mancate le proposte su come organizzare i repository istituzionali, gli archivi cui destinare i lavori da pubblicare.⁷ In Italia il maggior lavoro

⁴ M. Pietrangelo, *op. cit.*, 181.

⁵ Raccomandazione della Commissione del 17 luglio 2012 sull’accesso all’informazione scientifica e sulla sua conservazione (2012/417/UE., punto 1 del “si raccomanda”.

⁶ Le pubblicazioni scientifiche ammesse alla valutazione sono quelle espressamente elencate e definite nel D.P.R. 23 marzo 2000, n. 117, Regolamento recante modifiche al D.P.R. 19 ottobre 1998, n. 390, concernente le modalità di espletamento delle procedure per il reclutamento dei professori universitari di ruolo e dei ricercatori a norma dell’articolo 1 della legge 3 luglio 1998, n. 210.

⁷ Si tratta della oramai ben conosciuta “Dichiarazione di Berlino per l’accesso aperto alla letteratura scientifica”, che risale al 2003 e alla quale – secondo quanto si legge nel sito web della CRUI (Conferenza dei Rettori delle Università italiane; www.cruui.it) – attualmente hanno aderito 71 atenei. A partire dal sito della CRUI è possibile accedere all’area tematica dedicata alle biblioteche, all’interno della quale sono consultabili i documenti elaborati nell’ambito del Gruppo di lavoro per l’Open Access, istituito nel 2006.

è stato svolto nell'ambito della CRUI (Conferenza dei Rettori delle Università Italiane), che ha istituito all'interno della propria Commissione Biblioteca un Gruppo di lavoro per l'Open Access. I documenti elaborati in senso a questo Gruppo di lavoro sono tutti disponibili online; essi tracciano le "linee guida" per un percorso di avvicinamento al metodo dell'accesso aperto.

Accurate e circostanziate sono le proposte e le riflessioni presenti in questa ricca documentazione, dalle linee guida sul modello organizzativo e sulla metodologia per la costruzione di repository o archivi istituzionali; a quelle sulla gestione delle riviste elettroniche; a quello, più recente, sulla creazione e gestione dei metadati nei repository istituzionali etc.

Ma queste proposte non sono esenti dalla domanda che ho posto come preliminare. Come il nostro ordinamento qualifica questi archivi; e, se privi di considerazione a livello normativo, quali interventi di carattere regolatorio si rendono necessari perché le pubblicazioni in essi contenute siano equiparate a quelle tradizionali?⁸

Secondo le Linee guida in materia di Open Access, elaborate dal ricordato Gruppo di lavoro, "il ruolo che l'Open Access può avere nell'ambito della valutazione della ricerca riguarda la possibilità di sottoporre a giudizio anche *materiali non tradizionali* [corsivo mio] e di elaborare nuovi indicatori bibliometrici da affiancare a quelli attualmente in uso"⁹, quindi in definitiva si tratterebbe di affiancare al metodo tradizionale di pubblicazione il metodo dell'Open Access, che consisterebbe in un "valore aggiunto"¹⁰ per i processi di valutazione della ricerca.

Secondo la Dichiarazione di Berlino è necessario che l'Anagrafe istituzionale della ricerca (cioè la base dati che dovrebbe raccogliere, gestire ed elaborare tutte le informazioni su tutte le attività di ricerca) comprenda in sé gli Archivi istituzionali della ricerca, nei quali però i lavori devono essere pubblicati in versione completa e secondo standard di formato che ne consentano la massima integrazione.

Ma quali sono le caratteristiche di una Rivista Open Access? Questa la definizione di un *Open Access Journal* secondo la *Directory of Open Access Journals* (DOAJ): "We define open access journals as journals that use a funding model that does not charge readers or their institutions for access. From the BOAI (Budapest Open Access Initiative, ndr) definition of 'open access', we support the rights of users to 'read, download, copy, distribute, print, search, or link to the full texts of these articles' as mandatory for a journal to be included in the directory."¹¹ Anche in questo caso, dunque, esattamente come nel caso delle Riviste "tradizionali", cioè pubblicate a stampa da un editore, ciò che rileva è la qualità dei contenuti, la loro valutazione, il controllo sui testi e sulla loro scientificità.¹²

Non mi dilungo oltre sul tema, su cui la letteratura è estesa, giacché desidero arrivare subito al punto che mi preme indagare. E cioè, cosa ancora impedisce al nostro ordinamento di accogliere le pubblicazioni in Open Access tra quelle sussumibili e valutabili nelle procedure di valutazione della ricerca? Cioè, più precisamente, qual è il limite giuridico, se c'è, che impedisce una equipara-

⁸ In tale senso P. Guarda, *L'Open Access per la dottrina giuridica e gli Open Archives: verso un futuro migliore?*, in *Informatica e diritto*, 2, 2012, p. 227.

⁹ V. sul punto CRUI, *L'Open Access e la valutazione cit.*, p. 9, in particolare il dibattito richiamato nella nota 15.

¹⁰ *Ibidem*.

¹¹ www.doaj.org.

¹² *Ivi*.

zione dell'Open Access alle altre forme di disseminazione dei risultati della ricerca, senza ridurlo ad una forma – dunque in in sè non autonoma - di *pre* o *post print*?

2. L'Open Access nella più recente normativa statale

Partirei dalla più recente normativa in materia, che risale all'agosto del 2013, la quale, a prima lettura, sembra porsi in discontinuità con il precedente quadro regolatorio e in linea con le raccomandazioni della Commissione europea.

Precisamente, il riferimento è al decreto-legge 8 agosto 2013, n. 91, convertito con modifiche nella legge 7 ottobre 2013, n. 112,¹³ il cui articolo 4, rubricato “Disposizioni urgenti per favorire lo sviluppo delle biblioteche e degli archivi e per la promozione della recitazione e della lettura”, al comma secondo, così dispone: “Le pubblicazioni che documentano i risultati di ricerche finanziate per una quota pari o superiore al cinquanta per cento con fondi pubblici, indipendentemente dal formato della prima pubblicazione e dalle modalità della sua distribuzione o messa a disposizione del pubblico, devono essere depositate, *non oltre sei mesi dalla pubblicazione* [corsivo mio], in archivi elettronici istituzionali o di settore, predisposti in modo tale da garantire l'accesso aperto, libero e gratuito, dal luogo e nel momento scelti individualmente, l'interoperabilità all'interno e all'esterno dell'Unione Europea e la conservazione a lungo termine in formato elettronico. I soggetti preposti all'erogazione o alla gestione dei finanziamenti adottano le misure necessarie per l'attuazione dell'accesso aperto ai risultati della ricerca finanziata con fondi pubblici”.

Questo secondo comma dell'articolo 4 è stato modificato durante l'esame parlamentare per la conversione del decreto-legge: esso è stato interamente sostituito da un nuovo testo durante l'esame di merito nella settima Commissione del Senato.¹⁴

Questo il nuovo testo, oggi in vigore: “2. I soggetti pubblici preposti all'erogazione o alla gestione dei finanziamenti della ricerca scientifica adottano, nella loro autonomia, le misure necessarie per la promozione dell'accesso aperto ai risultati della ricerca finanziata per una quota pari o superiore al 50 per cento con fondi pubblici, quando documentati in articoli pubblicati su periodici a carattere scientifico che abbiano almeno due uscite annue. I predetti articoli devono includere una scheda di progetto in cui siano menzionati tutti i soggetti che hanno concorso alla realizzazione degli stessi. L'accesso aperto si realizza: a) tramite la pubblicazione da parte dell'editore, al momento della prima pubblicazione, in modo tale che l'articolo sia accessibile a titolo gratuito dal luogo e nel momento scelti individualmente; b) tramite la ripubblicazione senza fini di lucro in archivi elettronici istituzionali o disciplinari, secondo le stesse modalità, *entro diciotto mesi* [corsivo

¹³ Legge pubblicata nella Gazzetta Ufficiale n. 236 del 8 ottobre 2013 (testo coordinato nella G.U. n. 236 del 8 ottobre 2013). Per i lavori preparatori, cfr. XVII Legislatura, S1014/C1628 (Conversione in legge del decreto-legge 8 agosto 2013, n. 91, recante disposizioni urgenti per la tutela, la valorizzazione e il rilancio dei beni e delle attività culturali e del turismo), approvato in via definitiva il 3 ottobre 2013 con il nuovo titolo “Conversione in legge, con modificazioni, del decreto-legge 8 agosto 2013, n. 91, recante disposizioni urgenti per la tutela, la valorizzazione e il rilancio dei beni e delle attività culturali e del turismo”.

¹⁴ AS 1014, XVII Legislatura. Cfr. l'esame in sede referente nella 7a Commissione (Istruzione pubblica, beni culturali) del Senato. L'emendamento approvato, sostitutivo del secondo comma dell'art. 4, è stato presentato a firma del sen. Giannini ed altri (n. 4.10., testo 2).

mio] dalla prima pubblicazione per le pubblicazioni delle aree disciplinari scientifico-tecnico-mediche e *ventiquattro mesi* [corsivo mio] per le aree disciplinari umanistiche e delle scienze sociali. 2-bis. Le previsioni del comma 2 non si applicano quando i diritti sui risultati delle attività di ricerca, sviluppo e innovazione godono di protezione ai sensi del codice di cui al decreto legislativo 10 febbraio 2005, n. 30.”.

Quindi, in definitiva, la disposizione presente nel testo originario del decreto-legge imponeva da subito il deposito nei repository Open Access, non oltre sei mesi dalla data della loro pubblicazione, qualunque essa fosse. Ma, con le modifiche al testo del decreto introdotte in Senato, i tempi per il deposito in modalità Open Access si sono notevolmente allungati.

Una modifica che appare a questo punto in contrasto con la già ricordata raccomandazione della Commissione sull'accesso all'informazione scientifica, come emerso anche nel corso dell'esame del disegno di legge di conversione alla Camera. Col fine di impegnare il Governo a correggere la ridetta discrepanza, l'Aula della Camera – che pure aveva testè confermato il nuovo testo adottato dal Senato – approvava allora, col parere favorevole del Ministro per i beni culturali, Massimo Bray, presente in Aula, un ordine del giorno proposto dal deputato Quintarelli. Precisamente la Camera impegnava “[...] il Governo a valutare l'opportunità di adeguare in tempi rapidi la normativa contenuta nel presente provvedimento alla raccomandazione della Commissione europea citata in premessa, ed in particolare rispetto ai tempi di accesso aperto alle pubblicazioni prodotte nell'ambito delle attività di ricerca.”¹⁵

Riassumendo, dunque, la Commissione europea raccomanda l'Open Access, come pure altri organismi che operano a livello sovranazionale;¹⁶ si tratta di un modello molto apprezzato anche dal mondo della ricerca, direttamente coinvolto. Purtroppo, il nostro ordinamento procede timidamente, come appena rilevato a proposito delle alterne vicende del decreto-legge n. 91 del 2013. Così, dapprima si tenta un “avvicinamento” istituzionale al nuovo modello, cogliendo al volo l'occasione di un decreto-legge in materia di beni culturali, con una disposizione *ad hoc* che introduce un vincolo con effetti immediati, tanto che a partire dal 9 agosto 2013 iniziava il conto alla rovescia per la ripubblicazione in Open Access. Anche se relativamente ad alcune – e non a tutte – pubblicazioni scientifiche. Nella sua formulazione originaria, infatti, la ripubblicazione riguardava solo le “pubblicazioni che documentano i risultati di ricerche finanziate per una quota pari o superiore al cinquanta per cento con fondi pubblici”. Escludendo così i risultati della cosiddetta ricerca di base, anch'essa in gran parte finanziata con fondi pubblici, se svolta presso università ed enti di ricerca pubblici. Successivamente, come già ricordato, nella fase di conversione in legge il decreto-legge veniva modificato in Commissione al Senato, nel senso di prevedere una dilatazione dei tempi della pubblicazione dei lavori scientifici nei repository Open Access, e senza alcuna disciplina transitoria che contemplasse una graduale applicazione della nuova normativa. E ancora, a seguire, nell'esame in Aula alla Camera, le modifiche introdotte al Senato venivano confermate, pur se unitamente ad un atto d'indirizzo che impegnava il Governo a correggere rapidamente il testo appena approvato, per adeguare la tempistica del deposito nei repository Open Access alle

¹⁵ XVII Legislatura, Camera dei deputati, Ordine del giorno in Assemblea su progetto di legge n. 9/01628/048, accolto nella seduta n. 90 del 3/10/2013.

¹⁶ Tra gli altri, v. UNESCO (by A. Swan), *Policy guidelines for the development and promotion of open access*, 2012; UNESCO, *Institutional Repository Software Comparison*, 2014.

indicazioni dell'Unione europea.

Un *iter* faticoso e contraddittorio, che esprime a pieno quella resistenza del nostro ordinamento, di cui si diceva in principio.¹⁷

Un ramo del Parlamento (la Camera) impegna il Governo ad adeguare nei contenuti una normativa (disegno di legge di conversione di un decreto-legge), che pure è in corso di approvazione proprio in Parlamento, di fatto riproponendo una formulazione già adottata dallo stesso Governo (versione originaria del d.l.) e poi modificata dall'altro ramo del Parlamento (il Senato): una “tela di Penelope”, per citare una metafora già utilizzata a proposito delle nostre istituzioni e della qualità della regolazione da esse prodotta.¹⁸

3. Per concludere. Dalle resistenze giuridiche alle possibili vie di fuga

Quella appena descritta è, a mio avviso, l'ultima tessera di un quadro regolatorio per molti versi lacunoso, per altri versi, come detto, contraddittorio. A onor del vero, non che la raccomandazione della Commissione sia cristallina in ogni sua parte; il tipo di atto, infatti, si presta alla ricchezza di suggestioni, al punto tale da apparire in taluni passaggi ugualmente contraddittorio; o semplicemente incline ad assecondare i più diversi, e talora contrastanti, interessi. Così si raccomanda la tutela del ricercatore e della libertà della ricerca, ad esempio attraverso premi ai ricercatori che aderiscono all'Open Access, come ricordato in principio; la tutela degli editori, prevedendo anche accordi che consentono l'accesso sia all'abbonamento tradizionale sia a quello elettronico (pur sempre quindi ad un abbonamento); la tutela dei “meno fortunati”, come le piccole e medie imprese e i ricercatori “non affiliati”, per i quali devono essere previste condizioni di abbonamento più economiche (ancora un abbonamento).

Dinnanzi ad una regolazione incerta, ai diversi livelli di produzione, occorre chiedersi innanzitutto se le regole siano necessarie; se esse servano per mettere ordine in una prassi disomogenea, che rischia quindi – proprio perché non omogenea - di produrre lesioni nella sfera dei diritti dei singoli ricercatori, siano essi attivi, cioè produttori di conoscenza, siano essi passivi, cioè fruitori dei risultati delle ricerche altrui; e ancora, se di regole c'è bisogno, quale sia il livello di intervento più adeguato.

Si tratta di questioni complesse, sulle quali avevo tentato una prima parziale riflessione tempo addietro, muovendo proprio dall'esame delle norme che nel nostro ordinamento disciplinano la valutazione delle pubblicazioni scientifiche. In definitiva, all'epoca mi chiedevo se, di fronte ad una normativa risalente nel tempo e ad una giurisprudenza ad essa strettamente conforme, non vi fossero margini di autonomia nella regolazione della materia, pur nel rispetto del dettato norma-

¹⁷ Sfuggono a prima lettura le criticità della cattiva normazione; v. ad esempio A. De Robbio, *L'Open Access è legge anche in Italia*, in *Il giornale dell'Università degli studi di Padova “il Bo”*, 25 ottobre 2013, <http://www.unipd.it/ilbo/content/lopen-access-e-legge-anche-italia>.

¹⁸ L'allusione è al noto volume di A. Natalini, G. Tiberi (a cura di), *La tela di Penelope. Primo rapporto Astrid sulla semplificazione legislativa e burocratica*, Bologna, Il Mulino, 2010.

tivo, per i principali produttori di pubblicazioni scientifiche, cioè le università e gli enti pubblici di ricerca. Spazi di regolazione attraverso cui colmare quel vuoto normativo, che attraverso il riconoscimento dei lavori in Open Access, avesse potuto dare rilevanza e valore giuridico anche a tali lavori. Questa considerazione mi era stata sollecitata dalla lettura di alcune pronunce di tribunali amministrativi regionali nelle quali si argomentava a proposito della impossibilità di ammettere alla valutazione nei pubblici concorsi pubblicazioni scientifiche prive dei requisiti richiesti dalla normativa vigente in materia, e non menzionate tra quelle valutabili nei bandi di concorso dei singoli atenei. I quali bandi, com'è noto, di norma si limitano a riprodurre al proprio interno il testo della normativa in materia, e dunque gli elenchi delle pubblicazioni scientifiche presentabili *ex lege*, senza da essa discostarsi.

Com'è già ricordato, nell'ambito della CRUI opera la Commissione biblioteca, al cui interno è stato istituito il gruppo di lavoro sull'Open Access. Proprio i lavori di questo gruppo di studio hanno fortemente sensibilizzato le università sul tema dell'Open Access, tanto che quasi tutte (ben settantuno) hanno sottoscritto la nota dichiarazione di Berlino, aderendo quindi ai principi in essa indicati. Di queste, tuttavia, ben poche sono quelle che hanno dato seguito a tale adesione con un impegno più stringente, prevedendo cioè un espresso riferimento all'Open Access nei propri statuti, pur se con disposizioni di principio.¹⁹

¹⁹ Decreto 4 settembre 2012 dell'Università degli Studi del Piemonte Orientale (Modifica dello Statuto).

Art. 23 (Sistema bibliotecario di Ateneo e Commissione per le biblioteche), co. 4.

4. *Con apposito regolamento si prevedono le norme e le procedure finalizzate a dare piena attuazione all'accesso aperto alla letteratura scientifica e per assicurare la più ampia diffusione possibile dei risultati della ricerca nel rispetto della tutela della proprietà intellettuale e degli accordi in atto con enti e soggetti pubblici e privati.*

Decreto 8 giugno 2012 dell'Università della Tuscia (Modificazioni allo Statuto).

Art. 15 (Commissione Ricerca Scientifica di Ateneo), co. 1, lett. c).

1. *La Commissione Ricerca Scientifica svolge compiti istruttori, propositivi e consultivi per gli organi di governo dell'Ateneo su tutte le questioni riguardanti l'attività scientifica di Ateneo avvalendosi, ove opportuno, della collaborazione degli Uffici dell'Amministrazione centrale competenti e, eventualmente, di esperti.*

In particolare:

[...] c) *promuove la visibilità esterna della ricerca scientifica di Ateneo, anche attraverso l'incentivazione dell'accesso aperto ai prodotti della ricerca;*

Decreto 14 maggio 2012 dell'Università di Messina (Emanazione del nuovo statuto).

Art. 2, co. 4.

4. *L'Università degli studi di Messina fa propri i principi dell'accesso aperto alla letteratura scientifica e promuove la libera divulgazione in rete dei risultati delle ricerche prodotte in Ateneo, per assicurarne la più ampia diffusione possibile. Un apposito regolamento disciplina l'attuazione di tali principi nel rispetto delle leggi concernenti la proprietà intellettuale, la riservatezza e la protezione dei dati personali nonché la tutela, l'accesso e la valorizzazione del patrimonio culturale.*

Art. 7 (Strumenti per la ricerca scientifica), co. 3.

3. *La Scuola fa propri i principi dell'accesso aperto alla letteratura scientifica e promuove la libera diffusione dei risultati delle ricerche prodotte al suo interno.*

Decreto 19 aprile 2012 del Politecnico di Bari (Emanazione del nuovo statuto).

Art. 1 (Principi generali), co. 7.

7. *Il Politecnico promuove il principio dell'accesso aperto alla letteratura scientifica e la diffusione dei risultati della ricerca, nel rispetto della tutela della proprietà intellettuale.*

Decreto 29 marzo 2012 dell'Università "mediterranea" di Reggio Calabria (Emanazione dello statuto).

Art. 2 (Valori fondamentali), co. 2.

2. *L'Università Mediterranea fa propri i principi di accesso aperto alla letteratura scientifica e promuove la libera distribuzione in rete dei risultati delle ricerche prodotte in Ateneo, per assicurarne la massima diffusione possibile.*

Decreto 15 marzo 2012 dell'Università di Torino (Emanazione dello Statuto).

Art. 38 (Principi dell'accesso aperto)

1. *L'Università fa propri i principi dell'accesso pieno e aperto alla letteratura scientifica e promuove la libera disseminazione in rete dei*

Più interessante può forse risultare l'esame dei bandi di concorso, i quali però ad un primo esame non sembrano ammettere alla valutazione - nell'ambito delle singole procedure concorsuali - i lavori scientifici pubblicati in Open Access. E d'altro canto, come ricordato, il giudice amministrativo, continua ad attenersi strettamente alla norma, e dunque anch'esso non considera tale possibilità. Salvo manifestare apprezzamenti per l'Open Access, come di seguito si dirà.

Vien da chiedersi, ad esempio, perché mai gli atenei italiani non ammettano alla valutazione nelle procedure concorsuali tali pubblicazioni, vista l'adesione ai principi dell'Open Access.

Insiste su questo punto la Commissione europea, secondo cui occorre adeguare "il sistema di reclutamento e valutazione delle carriere dei ricercatori e il sistema di valutazione per l'assegnazione di finanziamenti ai ricercatori in modo che siano premiati coloro che aderiscono alla cultura di condivisione dei risultati di ricerca."²⁰ E ancora, sempre secondo la Commissione, "I sistemi migliorati dovrebbero tenere conto dei risultati della ricerca messi a disposizione in accesso aperto e sviluppare, promuovere e utilizzare nuovi modelli alternativi di valutazione delle carriere, nuovi

risultati delle ricerche prodotte in Ateneo, per assicurarne la più ampia diffusione possibile.

2. *L'Università, con apposito Regolamento, pone la disciplina finalizzata a dare attuazione ai principi dell'accesso pieno e aperto ai dati e ai prodotti della ricerca scientifica, incentivandone il deposito nell'archivio istituzionale e la comunicazione al pubblico, nel rispetto delle leggi concernenti la proprietà intellettuale, la riservatezza e la protezione dei dati personali, nonché la tutela, l'accesso e la valorizzazione del patrimonio culturale.*

Decreto 8 marzo 2012 dell'Università di Trieste (Emanazione del nuovo Statuto).

Art. 2 (Principi e garanzie fondamentali), co. 5.

5. *L'Università garantisce, nell'organizzazione delle attività di ricerca, l'indipendenza scientifica, la qualità dei risultati, la valorizzazione del merito, l'integrazione tra saperi e l'internazionalizzazione. L'Università riconosce l'accesso aperto alla letteratura scientifica; incentiva il deposito dei risultati della ricerca nei propri archivi istituzionali e ne promuove l'accessibilità, la circolazione e la divulgazione al pubblico nel rispetto delle leggi in materia di proprietà intellettuale, riservatezza e protezione dei dati personali. L'Università si impegna a conciliare i principi di accesso aperto alla letteratura scientifica e di diffusione dei risultati con la proprietà intellettuale. Sulla base dei risultati della ricerca, l'Università favorisce il trasferimento di conoscenze, anche per iniziative di impresa.*

Decreto 27 febbraio 2012 dell'Università di Pisa (Emanazione del nuovo statuto).

Articolo 38 (Il sistema bibliotecario e il sistema museale di ateneo), co. 1.

1. *Il sistema bibliotecario di Ateneo è un sistema unitario e coordinato delle strutture bibliotecarie e documentali dell'Università di Pisa preposte allo sviluppo, alla gestione, alla fruizione, alla valorizzazione e alla conservazione del patrimonio bibliografico e documentale. In particolare cura l'organizzazione dei servizi atti a favorire e promuovere l'accesso all'informazione bibliografica e la disseminazione della conoscenza attraverso le modalità tradizionali e mediante l'utilizzo delle nuove tecnologie e il sostegno all'accesso aperto alla letteratura scientifica di ogni ambito disciplinare, in funzione dell'esigenza della ricerca, della didattica e delle attività degli organi amministrativi e di valutazione dell'Ateneo. Il sistema bibliotecario di ateneo è costituito dalle biblioteche dell'Università e dall'archivio centrale di Ateneo. L'elenco di dette biblioteche e le norme generali per il funzionamento e la loro interconnessione sono definiti nel regolamento generale di Ateneo.*

Decreto 16 febbraio 2012 dell'Università degli studi di Bergamo (Emanazione dello Statuto).

Art. 2 (Attività didattica, di ricerca e internazionalizzazione), co. 10.

10. *L'Università fa propri i principi dell'accesso aperto alla letteratura scientifica e promuove la libera disseminazione in rete dei risultati delle ricerche prodotte in Ateneo, anche incentivandone il deposito nell'archivio istituzionale, nel rispetto delle leggi concernenti la proprietà intellettuale, la riservatezza e la protezione dei dati personali, nonché la tutela, l'accesso e la valorizzazione del patrimonio culturale.*

Decreto 29 dicembre 2011 dell'Università del Salento (Emanazione del nuovo Statuto).

Art. 1 (Principi generali), co. 7.

7. *L'Università promuove il principio dell'accesso aperto alla letteratura scientifica, nel rispetto delle leggi concernenti la proprietà intellettuale, la riservatezza, la tutela e la valorizzazione del patrimonio culturale.*

Decreto 29 febbraio 2012 dell'Università degli studi di Ferrara (Emanazione dello Statuto).

Art. 43 (Valutazione della ricerca), co. 3.

3. *Unife promuove la diffusione delle pubblicazioni scientifiche prodotte da soggetti operanti nell'Ateneo, attraverso gli strumenti più idonei e condivisi nella comunità scientifica nazionale e internazionale, inclusi quelli ad accesso aperto, laddove possibile.*

²⁰ Raccomandazione 2012/417/UE *cit.*, punto 2 del "si raccomanda".

criteri di misurazione e nuovi indicatori.”²¹ Com'è noto, si tratta di raccomandazioni, il cui valore persuasivo testimonia l'opera di mediazione tra gli interessi dell'editoria tradizionale, da un lato, e quelli della comunità scientifica, dall'altro. Si colloca in questo percorso istituzionale di avvicinamento ai principi dell'Open Access anche la l'avvio di una nuova infrastruttura per la ricerca predisposta in ambito comunitario, denominata OpenAIRE.eu, che consentirà di mettere a disposizione di chiunque il 20% delle ricerche finanziate dal 7° programma quadro, che nel complesso ammonta a 55 miliardi di euro. Il 7 PQ “riunisce tutte le iniziative dell'UE collegate alla ricerca che hanno un ruolo fondamentale per raggiungere gli obiettivi di crescita, competitività e occupazione, assieme a un nuovo Programma quadro per la competitività e l'innovazione (CIP), a programmi di istruzione e formazione, ai Fondi strutturali e ai Fondi di coesione per la convergenza regionale e la competitività. Inoltre è un pilastro fondamentale per lo Spazio europeo della ricerca (SER).”²². I lavori saranno resi disponibili su Openaire.eu dopo un embargo di sei o dodici mesi dalla pubblicazione sulle riviste scientifiche per tutelare il lavoro di selezione compiuto dagli editori.

Come anticipato, il nostro tema inizia a costituire “oggetto di riflessione” anche nelle aule dei Tribunali amministrativi, nel contenzioso in materia di concorsi pubblici.²³ Si tratta, però, di sensibilità isolate, che nulla possono dinanzi alle resistenze presenti nella nostra regolazione, come bene testimoniato proprio dagli stessi giudici amministrativi, i quali si limitano a verificare il rispetto dei criteri di ragionevolezza e di imparzialità dell'amministrazione nei procedimenti valutativi, oltre che “la conformità delle valutazioni ai criteri predeterminati nel bando, le cui regole costituiscono il vincolo e dirigono l'azione amministrativa in ossequio al principio di parità di trattamento e quindi di imparzialità.”²⁴. Si apprezza particolarmente, infatti, in alcune pronunce, la chiara distinzione tra la nozione di “accessibilità del pubblico” e quella di “pubblicazione” scientifica. Scrive, ad esempio, il Tar Campania/Salerno a proposito delle tesi di dottorato: “[...] le tesi di dottorato, per espressa indicazione delle ‘Linee guida per il deposito delle tesi di dottorato negli archivi aperti’ della Conferenza dei Rettori dell'Università italiane, emanate nell'ottobre 2007, benché siano sottoposte al giudizio finale espresso dalla commissione giudicatrice che ne certifica i requisiti di originalità e di contributo al sapere, non subiscono tuttavia una valutazione ai fini della pubblicazione fatta da uno o più esperti, né sono sottoposte ad un autentico processo di ‘revisione paritaria’ tipico delle opere che si desidera destinare a pubblicazione scientifica.”. E ancora, sempre ragionando di tesi di dottorato: anche delle tesi di dottorato, il deposito “in archivi istituzionali aperti le rende in sostanza assimilabili ai ‘documenti diffusi tramite rete informatica’ (concernenti la produzione scientifica delle università, centri di ricerca e delle istituzioni culturali) ed, in quanto tali, ricadenti fra quelle opere oggetto di deposito legale la cui disciplina il legislatore si riserva di precisare in un futuro regolamento.”²⁵

Insomma, come sembra aver ben chiaro questo giudice amministrativo, occorre distinguere tra i risultati della ricerca, i quali tutti dovrebbero essere resi accessibili al pubblico negli archivi isti-

²¹ *Ivi*.

²² European Commission, *Open Access Pilot in FP7*, 2008. In generale, v. i documenti pubblicati in http://ec.europa.eu/research/science-society/open_access.

²³ Cfr. T.A.R. Campania Salerno, Sez. I, 23 maggio 2011, n. 953.

²⁴ Sentenza TAR Campania Sez. Salerno *cit.*, punto 1 della motivazione.

²⁵ *Ivi*.

tuzionali Open Access, tra i risultati che non costituiscono oggetto di pubblicazione scientifica e quelli che invece integrano una pubblicazione scientifica.

Ma quale è il criterio che consente di effettuare questa distinzione? L'unico possibile riguarda il diverso livello di valutazione, che mancherebbe nel caso dei prodotti della ricerca diversi dalle “vere e proprie” pubblicazioni scientifiche (per esempio le tesi di dottorato), e invece sarebbe presente nel caso di testi sottomessi alla valutazione mediante il metodo peer review o altri metodi, adottati dalle riviste scientifiche, comprese quelle Open Access.

Resta ferma l'assenza di un solido e chiaro ancoraggio normativo, in assenza del quale permane la timidezza dei bandi di selezione e di concorso pubblici, che per l'appunto fanno riferimento – come già detto, con richiami pedissequi – proprio alla regolazione in materia, e cioè ai diversi decreti ministeriali.

La stessa CRUI, in una recente dichiarazione sull'accesso aperto, in fondo, al di là delle incongruenze della regolazione, che puntualmente sottolinea, se, da un lato, si spinge fino a suggerire “soluzioni operative”, ipotizzando il rafforzamento della posizione degli autori anche attraverso la previsione di nullità di clausole contrattuali “che escludano il riutilizzo, entro un ragionevole termine dalla prima pubblicazione, dell'opera pubblicata quale esito di ricerche prevalentemente finanziate con fondi pubblici”²⁶; dall'altro, in definitiva, auspica “azioni coordinate e concertate fra i diversi soggetti interessati, pubblici e privati, e fra le diverse sedi decisionali e operative.”²⁷.

La norma, dunque, può sì essere efficace, ma solo se ha alle spalle una convinta e condivisa scelta di tipo culturale e politico.

²⁶ CRUI, *L'accesso aperto alle pubblicazioni scientifiche*, gennaio 2014, in www.cru.it, p. 2.

²⁷ *Ibidem*, p. 3

L'EVOLUZIONE DEL MODELLO DI AMMINISTRAZIONE DIGITALE: DALL'E-GOVERNMENT ALL'OPEN GOVERNMENT

Fernanda Faini

 *Multimedia*



Clicca sull'immagine o fotografa il QrCode
per accedere al Mediabook CLIOedu

Abstract: L'analisi della recente normativa mostra un'evoluzione del modello di amministrazione digitale, che dall'*e-government* si sviluppa per assumere le caratteristiche dell'*open government* grazie alla previsione di strumenti, che dopo essere entrati nel dibattito pubblico e scientifico, sono approdati nel quadro normativo italiano. L'*open government* risponde all'esigenza di un profondo cambiamento delle istituzioni che segua l'evolversi delle modalità di relazione, comunicazione e collaborazione della società.

In tale direzione la normativa degli ultimi anni ha tracciato gli strumenti necessari all'*open government* sotto il profilo della trasparenza, della partecipazione e della collaborazione, i pilastri sui quali si basa l'implementazione di un modello di amministrazione aperta. Nelle recenti disposizioni emergono i principi della trasparenza e dell'apertura dei dati (*open data*) fino all'apertura dei servizi per mezzo di rapporti basati sulla partecipazione degli utenti, anche attraverso il loro coinvolgimento nei processi decisionali con strumenti di *e-democracy*. Il principio di collaborazione trova forma nel virtuoso "combinato disposto" costituito da *cloud computing*, riuso e *open source* all'interno del sistema pubblico e si caratterizza nei rapporti con l'esterno per l'utilizzo degli strumenti del *web 2.0* e per la fisionomia di *smart communities*.

Gli effetti dell'*open government* sono stimabili in evidenti risparmi, maggiore efficienza e semplicità, migliore qualità, recupero di credibilità e fiducia nelle istituzioni. Le nuove tecnologie sono in grado di tradursi in nuovi servizi e soluzioni inedite a vantaggio della collettività. L'evoluzione verso un'amministrazione digitale aperta si traduce in una strategia per la crescita dell'Italia con l'effetto finale consistente nel guadagno complessivo del sistema Paese.

The analysis of recent legislation shows an evolution in the model of digital administration. This concept has begun to develop from *e-government* to assume the characteristics of *open government* through the provision of new tools, adopted in the Italian regulatory framework. The *open government* responds to the need for a profound change of the institutions, that has to follow the development of the methods of interaction, communication and collaboration of society.

The recent legislation has drawn the necessary tools to the *open government* in terms of transparency, participation and collaboration, the pillars on which is based the implementation of a model of *open government*. In these rules emerge the principles of transparency and openness of the data (*open data*) and the openness of services by means of relations based on user participation, also through their involvement in decision-making processes with tools of *e-democracy*. The principle of collaboration arises in the form of a virtuous "conjunction" consisting of *cloud computing*, reutilization and *open source* within the public system, and is characterized for the use of *web 2.0* tools and the features of the *smart communities* in the relations with the outside world.

The effects of the construction of *open government* are estimated at substantial savings, a greater efficiency and simplicity, an improved quality, the recovery of credibility and trust in institutions. The new technologies are able to arise in new services and innovative solutions for the benefit of the whole community.

The evolution towards an open digital administration results in a strategy for the growth of Italy with the final effect consisting in the overall gain for the whole Country.

Parole chiave: *open government*, amministrazione digitale, trasparenza, partecipazione, collaborazione, *open data*, inclusione digitale, servizi in rete, *customer satisfaction*, *e-democracy*, *cloud computing*, riuso, *open source*, *web 2.0*, *smart communities*.

Sommario: 1. L'evoluzione normativa verso l'amministrazione digitale aperta – 1.1 Dall'e-government all'open government – 1.2 I presupposti dell'open government – 2. Strumenti di open government – 3. Trasparenza e apertura – 3.1 L'amministrazione trasparente – 3.2 Gli open data – 3.3 Qualità delle informazioni e inclusione digitale – 4. Partecipazione – 4.1 Servizi in rete e customer satisfaction – 4.2 E-democracy – 5. Collaborazione – 5.1 Cloud computing, riuso, open source – 5.2 Il web 2.0 e le smart communities – 6. Gli effetti dell'open government.

1. L'evoluzione normativa verso l'amministrazione digitale aperta

La società contemporanea vive una profonda evoluzione, caratterizzata dall'impatto pervasivo delle nuove tecnologie su ogni aspetto individuale e sociale della vita e contraddistinta dal principio di *openness*, che permette facilità nell'acquisizione e trasmissione della conoscenza e favorisce un approccio “a rete” in grado di creare sinergie inedite tra i soggetti e di far emergere l'intelligenza collettiva¹.

Tale evoluzione della società origina dalla crescita delle informazioni disponibili e dal facile accesso alle stesse per mezzo della tecnologia, che di conseguenza comporta cambiamenti profondi nel modo di avere e di creare la conoscenza. Le tecnologie mutano le relazioni fra gli individui, che diventano semplici e immediate, in quanto vengono abbattuti gli ostacoli della distanza territoriale e temporale². Le attività private e pubbliche si spostano dalla realtà fisica a quella virtuale e le rappresentazioni informatiche sono produttive di effetti giuridici. La collettività si caratterizza sempre più come “società della rete”, in cui le tecnologie sono strumenti di uso quotidiano e le nuove parole d'ordine sono partecipazione, condivisione e collaborazione³.

La rinnovata fisionomia della società, seppur innescata dall'ingresso delle nuove tecnologie, in

¹ Secondo P. LÉVY, *L'intelligenza collettiva. Per un'antropologia del cyberspazio*, trad.it., Milano, Feltrinelli, 1996, p. 34 e seguenti l'intelligenza collettiva è “un'intelligenza distribuita ovunque, continuamente valorizzata, coordinata in tempo reale, che porta a una mobilitazione effettiva delle competenze. [...] Lungi dal fondere le intelligenze individuali in una sorta di magma indistinto, l'intelligenza collettiva è un processo di crescita, di differenziazione e di mutuo rilancio delle specificità. L'immagine dinamica che emerge dalle sue competenze, dai suoi progetti e dalle relazioni che i suoi membri intrattengono all'interno dello Spazio del sapere, costituisce per un collettivo una nuova modalità di identificazione, aperta, viva e positiva”. Come rileva F. DI DONATO, *Lo stato trasparente. Linked open data e cittadinanza attiva*, Pisa, Edizioni ETS, 2011, p. 82 l'intelligenza collettiva è prodotta dalla “compresenza della massima accessibilità dell'informazione e della massima libertà di accrescere la massa di queste informazioni”.

² Nella società dell'informazione, la “virtualità” comporta cambiamenti nel fattore “tempo”, dal momento che le tecnologie rendono sostanzialmente immediata la trasmissione delle comunicazioni. Inoltre si modifica il fattore “spazio”, in quanto la cosiddetta società della rete si caratterizza per l'aterritorialità, dal momento che le tecnologie permettono di prescindere dal vincolo territoriale e dalle distanze geografiche, configurandosi come presupposto e motore del fenomeno della globalizzazione. Cfr. G. SARTOR, *L'informatica giuridica e le tecnologie dell'informazione. Corso di informatica giuridica*, seconda edizione, Torino, Giappichelli, 2010, p. 1 e seguenti.

³ In tal senso G. SARTOR, *L'informatica giuridica e le tecnologie dell'informazione. Corso di informatica giuridica*, cit., p. 1 e seguenti. Lo sviluppo della società contemporanea è parallelo all'evoluzione in senso partecipativo di Internet con il passaggio dal *web 1.0* al *web 2.0*, che assicura un alto livello di interazione e si avvale in maniera sostanziale dei contributi degli utenti; cfr., più ampiamente, paragrafo 2.3.2.

queste non si esaurisce, dal momento che si deve tradurre in una conseguente e necessaria modifica delle logiche di azione. Ciò presuppone un profondo cambiamento culturale e organizzativo che deve unirsi a una reingegnerizzazione dei processi e delle attività.

Questo profondo sviluppo della società è all'origine dell'evoluzione dell'amministrazione pubblica nel senso dell'apertura, essenziale per rispondere efficacemente alle esigenze attuali della collettività. È quanto mai necessario che le istituzioni abbiano la capacità di parlare lo stesso linguaggio impiegato nella società, alla luce del fatto che le amministrazioni pubbliche trovano la stessa ragione d'essere nel realizzare il benessere della collettività.

Si tratta pertanto di impiegare i nuovi mezzi di comunicazione nelle politiche pubbliche, per assumere un atteggiamento atto a recepire l'intelligenza collettiva e destinarla al bene stesso della comunità, per mezzo di un nuovo approccio "orizzontale" caratterizzato dalla condivisione e dalla collaborazione delle istituzioni con cittadini, associazioni e imprese. Le tecnologie permettono quindi di dare sostanza all'innovazione in senso ampio, quale cambiamento di logiche e di processi dell'agire pubblico⁴.

Tale processo evolutivo, pertanto, ha interessato l'amministrazione pubblica, attore protagonista della società contemporanea, che vive questi profondi cambiamenti.

Di conseguenza l'amministrazione digitale (*e-government*)⁵ negli ultimi anni sta maturando, coniugandosi e sviluppandosi nell'*open government*, modello secondo cui i governi e le amministrazioni devono essere trasparenti a tutti i livelli e le loro attività aperte e disponibili per favorire così azioni efficaci e garantire un controllo pubblico del proprio operato mediante le nuove tecnologie⁶.

1.1 Dall'e-government all'open government

L'analisi della recente normativa mostra un'evoluzione del modello di amministrazione digitale, che dall'*e-government* si sviluppa per assumere le caratteristiche dell'*open government* grazie alla previsione di strumenti, che dopo essere entrati nel dibattito pubblico e scientifico, sono approdati nel quadro normativo italiano e hanno fatto acquisire all'amministrazione digitale italiana una più decisa configurazione aperta.

⁴ In tal senso e, più in generale, sull'*open government* cfr. F. FAINI, *La strada maestra dell'open government: presupposti, obiettivi, strumenti*, in "Cyberspazio e diritto", n. 2, 2013, pp. 213-240.

⁵ L'amministrazione digitale o *e-government* consiste nell'organizzazione delle attività dell'amministrazione pubblica fondata sull'adozione estesa e integrata delle tecnologie dell'informazione e della comunicazione nello svolgimento delle funzioni e nell'erogazione dei servizi, al fine di garantire azioni efficaci, accrescere la soddisfazione degli utenti, rafforzare il processo democratico e sostenere le politiche pubbliche. In tal senso la definizione di amministrazione elettronica contenuta nell'art. 3, comma 1, lett. a) della legge regionale toscana 26 gennaio 2004, n. 1, recante "Promozione dell'amministrazione elettronica e della società dell'informazione e della conoscenza nel sistema regionale. Disciplina della «Rete telematica regionale toscana»".

⁶ La data fondamentale per l'*open government* è individuata nell'8 dicembre 2009, momento del lancio dell'*Open Government Directive* da parte del Presidente degli Stati Uniti Barack Obama, che ha conferito un'accezione più contemporanea al concetto di trasparenza amministrativa: ha individuato negli *open data* uno strumento di partecipazione di cittadini e imprese alle scelte pubbliche e ha prescritto al tempo stesso alle agenzie pubbliche i principi della filosofia *open*: trasparenza, partecipazione e collaborazione. In merito cfr. E. BELISARIO, G. COGO, R. SCANO, *I siti web delle pubbliche amministrazioni. Norme tecniche e giuridiche dopo le Linee Guida Brunetta*, Rimini, Maggioli, 2011, p. 163 e seguenti.

In materia, negli ultimi anni si sono susseguiti interventi normativi, che hanno ricevuto impulso dalle politiche comunitarie e, in particolare, dall'Agenda digitale europea⁷.

Dopo la profonda riforma del d.lgs. 30 dicembre 2010, n. 235 che ha interessato quella che può essere considerata la *magna charta* in materia, ossia il codice dell'amministrazione digitale (di seguito anche CAD), di cui al d.lgs. 7 marzo 2005, n. 82, negli ultimi anni sono state approvate norme importanti come il cosiddetto decreto Semplificazioni (d.l. 9 febbraio 2012, n. 5 convertito con modificazioni dalla legge 4 aprile 2012, n. 35), che ha dato sostanza all'Agenda digitale italiana⁸, e il cosiddetto decreto Sviluppo 2012 (d.l. 22 giugno 2012, n. 83 convertito con modificazioni dalla legge 7 agosto 2012, n. 134), contenente significative disposizioni sull'"amministrazione aperta" e l'*open source*.

L'evoluzione normativa verso l'*open government* si è sostanziata poi nelle pervasive modifiche all'amministrazione digitale del cosiddetto decreto Crescita 2.0 (d.l. 18 ottobre 2012, n. 179 convertito con modificazioni dalla legge 17 dicembre 2012, n. 221) e, infine, ha trovato forma nel cosiddetto decreto Trasparenza, il d.lgs. 14 marzo 2013, n. 33 che, in attuazione della legge 6 novembre 2012, n. 190 (cosiddetta legge Anticorruzione), riordina le disposizioni in materia di pubblicità, trasparenza e diffusione delle informazioni.

Alle norme si sono accompagnate strategie politiche tradotte nei piani di azione per l'*e-government* e da ultimo nell'Agenda digitale italiana, cornice strategica degli obiettivi, azioni e interventi necessari a realizzare l'amministrazione digitale italiana, che si caratterizza sempre più per la fisionomia di *open government*⁹.

L'*open government*, che basa le sue fondamenta su apertura, trasparenza, collaborazione e partecipazione¹⁰, può dare sostanza a un'innovazione in senso ampio, al fine di attivare nella società nuova creatività, rinnovata competitività e innovazione sociale.

⁷ L'Agenda Digitale europea è una delle sette iniziative "faro" individuate nella più ampia Strategia Europea 2020, che mira a realizzare una crescita intelligente, sostenibile e inclusiva. L'Agenda digitale europea è orientata a stabilire un ruolo chiave delle tecnologie dell'informazione e della comunicazione per raggiungere gli obiettivi che l'Europa si è posta ed è finalizzata a sfruttare al meglio il potenziale delle tecnologie per favorire l'innovazione, la crescita economica e il progresso. Sulle strategie politiche e normative dell'Unione europea cfr. D. A. LIMONE, *Politica e Normativa Comunitaria per la Società dell'Informazione (1990-2010)*, in "Rivista elettronica di Diritto, Economia, Management", n. 1, 2010, rivista telematica in http://www.giuritecne.it/wp-content/uploads/2011/01/rivista-elettronica_1_2010.pdf.

⁸ L'Agenda digitale italiana è prevista nell'art. 47 del d.l. 5/2012 convertito con modificazioni dalla legge 35/2012.

⁹ I cosiddetti piani d'azione per l'*e-government* indicano le azioni necessarie per conseguire gli obiettivi previsti dalle norme, aggiungendo al sostegno politico anche la necessaria copertura economica. Alla prima fase del piano d'azione nazionale per l'*e-government* (dal 2000), è seguita la seconda fase (dal 2003) caratterizzata dalla strategia "L'*e-government* per un federalismo efficiente: una visione condivisa, una realizzazione cooperativa", per arrivare poi al piano di *e-gov* 2012 (presentato nel 2009). Attualmente si parla di Agenda digitale italiana, che si muove nel quadro dell'Agenda digitale europea e trova preciso riferimento normativo nell'art. 47 del decreto Semplificazioni (d.l. 5/2012 convertito con modificazioni dalla legge 35/2012).

¹⁰ In E. BELISARIO, G. COGO, R. SCANO, *I siti web delle pubbliche amministrazioni. Norme tecniche e giuridiche dopo le Linee Guida Brunetta*, cit., p. 163 e ss. si rileva come "nell'ambito dell'*e-Government* (e parallelamente alla diffusione del *web 2.0*) si è iniziata a fare strada la dottrina dell'*Open Government* (letteralmente "governo aperto") secondo cui l'amministrazione deve essere trasparente a tutti i livelli e consentire un controllo continuo del proprio operato mediante l'uso delle nuove tecnologie. [...] Centralità del cittadino, partecipazione, accesso universale ai dati, uso del *web* (e in particolare dei dispositivi mobili) sono i tratti distintivi dell'*Open Government*".

1.2 I presupposti dell'open government

L'*open government* presuppone un profondo cambiamento delle istituzioni sia dal punto di vista delle relazioni fra le diverse amministrazioni, sia dal punto di vista dei rapporti del sistema istituzionale con la società.

Per quanto attiene al primo profilo, il rapporto fra le istituzioni deve assumere la fisionomia della collaborazione, della condivisione dei dati, dei processi e degli obiettivi. E' importante pertanto realizzare la condivisione e lo scambio di dati e informazioni fra amministrazioni da un punto di vista tecnologico, ma è altresì necessario dare vita a una collaborazione di tipo progettuale, in cui la regola sia lo scambio di soluzioni e buone pratiche tra amministrazioni diverse.

Si tratta di costruire un sistema pubblico che, pur nelle necessarie differenziazioni, realizzi un'amministrazione uniforme e omogenea indipendentemente dalla collocazione geografica, dalla dimensione o dalla tipologia, semplificando la fruizione per gli utenti non più costretti a comprendere diversi linguaggi e differenti modalità operative.

Dal punto di vista dei rapporti con la società, *openness* significa innanzitutto servirsi del principio costituzionale della sussidiarietà orizzontale, favorendo l'autonoma iniziativa dei cittadini, singoli e associati, per lo svolgimento di attività di interesse generale¹¹. Vuol dire poi sviluppare una proficua "contaminazione" fra mondo pubblico e privato nelle attività e nei servizi pubblici, grazie anche agli strumenti collaborativi del *web 2.0*.

Ciò si traduce nella revisione di processi e modelli di azione e nell'elaborazione di soluzioni inedite, nell'ottica suggerita dall'Europa, che prevede come priorità l'*empowerment* di cittadini e imprese, ossia il coinvolgimento e la produzione collaborativa di servizi¹². La società composta da imprese, *startup*, associazioni, esperti e semplici utenti può offrire un grande apporto in tal senso, al fine di realizzare servizi funzionali e idonei a rispondere efficacemente alle esigenze della collettività.

Questa logica che caratterizza l'*open government*, per mezzo dei recenti interventi normativi, arriva a plasmare il modello originario di amministrazione digitale.

2. Strumenti di open government

Quali strumenti di amministrazione digitale aperta sono previsti o incentivati dalle norme? Quali previsioni normative hanno comportato l'evoluzione dal modello di *e-government* a quello di *open go-*

¹¹ Il principio di sussidiarietà orizzontale trova fondamento costituzionale nell'art. 118, comma 4, Costituzione. Sul principio di sussidiarietà digitale orizzontale cfr. M. MANCARELLA, *La Società dell'Informazione tra eGovernment e principio di sussidiarietà*, in "Rivista elettronica di Diritto, Economia, Management", n. 1, 2010, rivista telematica in http://www.giuritecne.it/wp-content/uploads/2011/01/rivista-elettronica_1_2010.pdf.

¹² Nel piano d'azione europeo per l'*e-government* 2011-2015, adottato nel 2010, tra le priorità si prevede l'*empowerment* degli utenti, ossia una responsabilizzazione tesa a incrementare nei cittadini, nelle imprese e in altre organizzazioni la capacità di essere proattivi nella società mediante il ricorso a nuovi strumenti tecnologici. A tale proposito sono previste come linee di azione lo sviluppo di servizi progettati per rispondere alle esigenze degli utenti e di servizi inclusivi, una produzione collaborativa di servizi (ad esempio con strumenti del *web 2.0*), il riutilizzo di informazioni nel settore pubblico, il miglioramento della trasparenza, il coinvolgimento di cittadini e imprese nei processi decisionali (*e-democracy*).

vernment? La risposta si trova nella normativa italiana degli ultimi anni che ha delineato gli strumenti necessari all'*open government* sotto i profili della trasparenza, della partecipazione e della collaborazione, i tre pilastri sui quali si basa l'implementazione di un modello di amministrazione aperta. Per realizzare un effettivo *open government* è, infatti, necessario far coesistere un insieme di elementi fondanti, che discendono dalle esaminate caratteristiche relazionali nuove che il soggetto pubblico deve assumere. Questi elementi vanno a toccare l'intera fisionomia e l'intima natura dell'amministrazione pubblica, dal momento che riguardano non solo il suo funzionamento interno, ma anche il volto che guarda all'esterno, tracciando un nuovo concetto di trasparenza e prevedendo la realizzazione di servizi maggiormente biunivoci, la cui ricchezza sta proprio nell'apporto partecipativo e collaborativo esterno.

In specifico i principi fondamentali dell'*open government*, ossia trasparenza, partecipazione e collaborazione, trovano linfa in strumenti giuridici introdotti o incentivati dalla normativa recente, che saranno oggetto di analisi.

3. Trasparenza e apertura

3.1 L'amministrazione trasparente

Il principio di trasparenza ha conosciuto un crescente interesse nei suoi confronti da parte della normativa, particolarmente accentuato negli ultimi anni.

Strumento atto a garantire il buon andamento e l'imparzialità della pubblica amministrazione, la trasparenza trova centralità già nella legge 7 agosto 1990, n. 241, come modificata nel 2005, in cui si pone come principio dell'attività amministrativa, accanto ai criteri di economicità, efficacia, imparzialità e pubblicità¹³. Emerge la natura della trasparenza non solo come garanzia di accesso per coloro che ne hanno diritto¹⁴, ma altresì quale accessibilità che prescinde dalla sfera giuridica di determinati soggetti ed è idonea ad assicurare una conoscenza diffusa e generale delle informazioni¹⁵.

Il principio di trasparenza consente l'attribuzione a cittadini e imprese di un potere di controllo democratico sull'operato delle istituzioni, che si coordina con l'esigenza di una pubblica amministrazione *customer oriented*, idonea a garantire all'utente un ruolo attivo di partecipazione alle deci-

¹³ Art. 1, comma 1, legge 241/1990, come modificato dalla legge 11 febbraio 2005, n. 15 e dalla legge 18 giugno 2009, n. 69.

¹⁴ Il Capo V (art. 22 e seguenti) della legge 241/1990 è dedicato al diritto di accesso ai documenti amministrativi. Il diritto di accesso consiste nel diritto degli interessati di prendere visione e di estrarre copia di documenti amministrativi (art. 22, comma 1, lett. a), legge 241/1990); spetta a tutti i soggetti privati, compresi quelli portatori di interessi pubblici o diffusi, che abbiano un interesse diretto, concreto e attuale, corrispondente ad una situazione giuridicamente tutelata e collegata al documento al quale è chiesto l'accesso (art. 22, comma 1, lett. b), legge 241/1990). La richiesta di accesso deve essere motivata e deve essere rivolta all'amministrazione che ha formato il documento e che lo detiene stabilmente (art. 25, comma 2, legge 241/1990).

¹⁵ L'aspetto di comunicazione e pubblicazione del patrimonio informativo pubblico verrà poi ampiamente trattato dalla successiva legge 7 giugno 2000, n. 150, relativa alle attività di informazione e comunicazione delle pubbliche amministrazioni.

sioni e alle attività pubbliche.

Le caratteristiche della trasparenza necessariamente le fanno trovare un forte alleato nelle nuove tecnologie, in Internet e nel *web*, capaci di rendere l'informazione disponibile a un numero indefinito di soggetti e consultabile in ogni momento da luoghi fisici diversi, caratteristiche oggi accentuate grazie alla possibilità di accesso da diversi *device* (quali pc fissi e portatili, *tablet*, *smartphone*).

Di conseguenza la trasparenza ha caratterizzato fortemente il codice dell'amministrazione digitale, d.lgs. 82/2005, ponendosi come finalità principale e permeandone le disposizioni; è stata poi accentuata da successivi interventi normativi, che hanno aumentato l'insieme delle informazioni oggetto di pubblicazione obbligatoria sul *web*¹⁶.

Fra questi interventi la legge 18 giugno 2009, n. 69 non si è limitata ad aumentare le informazioni oggetto di pubblicazione obbligatoria, ma ha anche previsto che gli obblighi di pubblicazione di atti e provvedimenti amministrativi aventi effetto di pubblicità legale si intendono assolti con la pubblicazione nei propri siti informatici da parte delle amministrazioni: di conseguenza le pubblicazioni effettuate in forma cartacea non hanno più effetto di pubblicità legale¹⁷.

Successivamente la c.d. Riforma Brunetta (di cui alla legge delega 4 marzo 2009, n. 15 e al relativo d.lgs. 27 ottobre 2009, n. 150), con particolare riferimento all'organizzazione e alla gestione del personale pubblico, ha statuito il concetto di *total disclosure*, accessibilità totale delle informazioni coniugata alla finalità di favorire forme diffuse di controllo del rispetto dei principi di buon andamento e imparzialità¹⁸.

In seguito sono state emanate regole, direttive e linee guida finalizzate a favorire trasparenza e apertura definendo caratteristiche e contenuti del sito *web*, porta di accesso virtuale al patrimonio informativo delle amministrazioni pubbliche¹⁹.

¹⁶ Fra gli interventi normativi successivi al d.lgs. 82/2005, ha aumentato il novero dei dati la cui pubblicazione sul sito *web* è obbligatoria la legge 18 giugno 2009, n. 69 "Disposizioni per lo sviluppo economico, la semplificazione, la competitività nonché in materia di processo civile", in particolare artt. 21, 23, comma 5, e 32.

¹⁷ Così art. 32 legge 69/2009, che lascia ferma la possibilità per le amministrazioni e gli enti pubblici, in via integrativa, di effettuare la pubblicità sui quotidiani a scopo di maggiore diffusione, nei limiti degli ordinari stanziamenti di bilancio.

¹⁸ In specifico la normativa si riferisce alle informazioni concernenti ogni aspetto dell'organizzazione delle pubbliche amministrazioni, degli indicatori relativi agli andamenti gestionali e all'utilizzo delle risorse per il perseguimento delle funzioni istituzionali, dei risultati dell'attività di misurazione e valutazione svolta in proposito dagli organi competenti. Si tratta in particolare dell'art. 4, comma 7, legge 15/2009 "Delega al Governo finalizzata all'ottimizzazione della produttività del lavoro pubblico e alla efficienza e trasparenza delle pubbliche amministrazioni nonché disposizioni integrative delle funzioni attribuite al Consiglio nazionale dell'economia e del lavoro e alla Corte dei conti" e dell'art. 11, comma 1, d.lgs. 150/2009 "Attuazione della legge 4 marzo 2009, n. 15 in materia di ottimizzazione della produttività del lavoro pubblico e di efficienza e trasparenza delle pubbliche amministrazioni" (l'art. 11 del d.lgs. 150/2009 è stato abrogato dal d.lgs. 33/2013).

¹⁹ Senza pretesa di esaustività, la direttiva n. 8 del 26 novembre 2009, *Direttiva del Ministro per la pubblica amministrazione e l'innovazione per la riduzione dei siti web delle pubbliche amministrazioni e per il miglioramento della qualità dei servizi e delle informazioni online al cittadino*, le relative *Linee guida per i siti web della PA* del 26 luglio 2010, adottate in attuazione della direttiva 8/2009 e poi aggiornate nel 2011, la delibera n. 105 del 14 ottobre 2010 della Commissione Indipendente per la Valutazione, la Trasparenza e l'Integrità delle amministrazioni pubbliche (CiVIT), recante *Linee guida per la predisposizione del Programma triennale per la trasparenza e l'integrità*, poi la delibera CiVIT n. 2 del 5 gennaio 2012, recante *Linee guida per il miglioramento della predisposizione e l'aggiornamento del Programma triennale per la Trasparenza e Integrità* e, da ultimo, la delibera CiVIT n. 50 del 4 luglio 2013, recante *Linee guida per l'aggiornamento del Programma triennale per la trasparenza e l'integrità 2014-2016*. Alle *Linee Guida sui siti web* hanno fatto seguito anche una serie di *Vademecum sull'albo online* (2011), su *PA e social media* (2011), sugli *open data* (2011), sulla misurazione della qualità dei siti *web* (2012), ecc.

La stessa profonda modifica del d.lgs. 82/2005 recata dal d.lgs. 235/2010, che ha fatto parlare di nuovo codice dell'amministrazione digitale, ha inciso sugli strumenti con cui si garantisce la trasparenza, ampliandoli e cercando di conferire loro maggiore effettività²⁰.

Il percorso di apertura è culminato oggi nel cosiddetto decreto Trasparenza, il d.lgs. 33/2013, che, in attuazione della cosiddetta legge Anticorruzione (legge 190/2012), ha compiuto un corposo riordino degli obblighi di pubblicità, trasparenza e diffusione delle informazioni previsti da disposizioni che si erano susseguite e talvolta sovrapposte nel corso degli anni²¹.

Il decreto ha disposto il principio di pubblicità e il diritto alla conoscibilità di documenti, informazioni e dati oggetto di pubblicazione obbligatoria²², intendendo la trasparenza, in continuità con la Riforma Brunetta, come accessibilità totale delle informazioni concernenti l'organizzazione e l'attività delle pubbliche amministrazioni, allo scopo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche²³.

Le disposizioni del decreto Trasparenza sono dotate di particolare *vis* normativa, in quanto integrano l'individuazione del livello essenziale delle prestazioni erogate dalle amministrazioni pubbliche a fini di trasparenza, prevenzione, contrasto della corruzione e della cattiva amministrazione, a norma dell'art. 117, secondo comma, lettera m), Costituzione²⁴. Inoltre la trasparenza, ai sensi del decreto, concorre ad attuare il principio democratico e i principi costituzionali di eguaglianza, imparzialità, buon andamento, responsabilità, efficacia ed efficienza nell'utilizzo di risorse pubbliche, integrità e lealtà nel servizio alla nazione²⁵; nel decreto viene esplicitato che la trasparenza concorre alla realizzazione di un'amministrazione aperta al servizio del cittadino, pilastro quindi dell'implementazione di un modello di *open government*.

Il decreto Trasparenza ha riordinato gli obblighi, che si erano sommati nel corso degli anni, suddividendoli in macro-ambiti concernenti l'organizzazione e l'attività delle pubbliche amministrazioni, l'uso delle risorse pubbliche, le prestazioni offerte e i servizi erogati e, infine, i "settori speciali" (contratti pubblici di lavori, servizi e forniture; attività di pianificazione e governo del territorio;

²⁰ In merito cfr. F. FAINI, *Dati, siti e servizi in rete delle pubbliche amministrazioni: l'evoluzione nel segno della trasparenza del decreto legislativo n. 235 del 2010*, in D. TISCORNIA (a cura di), *Open data e riuso dei dati pubblici*, in "Informatica e diritto", n.1-2, 2011, pp. 263-286.

²¹ Si tratta del d.lgs. 33/2013, recante "Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni", adottato a seguito della delega di cui all'art. 1, commi 35 e 36, della legge 190/2012. Sull'attuazione del decreto Trasparenza la Presidenza del Consiglio dei ministri – Dipartimento della Funzione Pubblica ha approvato la circolare n. 2 del 19 luglio 2013, recante *D.lgs. n. 33/2013 – Attuazione della trasparenza*, in <http://www.funzionepubblica.gov.it>.

²² In specifico art. 3 del d.lgs. 33/2013.

²³ Art.1, comma 1, d.lgs. 33/2013.

²⁴ Art.1, comma 3, d.lgs. 33/2013, che precisa altresì che le disposizioni costituiscono esercizio della funzione di coordinamento informativo statistico e informatico dei dati dell'amministrazione statale, regionale e locale, di cui all'art. 117, secondo comma, lettera r), della Costituzione. In tal senso anche art. 1, comma 36, legge 190/2012. Le disposizioni rientrano pertanto nelle materie di competenza legislativa esclusiva dello Stato, che sono appunto previste dal comma secondo dell'art. 117 C.

²⁵ Art. 1, comma 2, d.lgs. 33/2013, ai sensi del quale ciò deve avvenire nel rispetto delle disposizioni in materia di segreto di Stato, di segreto d'ufficio, di segreto statistico e di protezione dei dati personali. Secondo la disposizione inoltre la trasparenza è condizione di garanzia delle libertà individuali e collettive, nonché dei diritti civili, politici e sociali e integra il diritto a una buona amministrazione.

servizio sanitario nazionale, ecc.)²⁶.

A fini di piena accessibilità, omogeneità e semplicità di fruizione, il decreto Trasparenza ha previsto e disciplinato una specifica sezione nella *home page* del sito *web* istituzionale, denominata “Amministrazione Trasparente”, in cui devono confluire i dati, le informazioni e i documenti oggetto di pubblicazione ai sensi della normativa vigente, dettagliandone organizzazione e struttura²⁷; si conferisce volto omogeneo alla trasparenza delle pubbliche amministrazioni grazie alla previsione di contenuti organizzati e strutturati in una veste grafica comune.

Al fine di assicurare effettività alle norme e permettere un controllo pubblico in merito, il d.lgs. 33/2013 ha previsto un nuovo istituto, l’accesso civico, con cui i cittadini possono richiedere documenti, informazioni e dati oggetto di pubblicazione obbligatoria nei casi in cui sia stata omessa la loro pubblicazione, senza nessuna limitazione quanto alla legittimazione soggettiva del richiedente, senza necessità di alcuna motivazione e gratuitamente²⁸.

Queste caratteristiche differenziano tale istituto dal diritto di accesso, già normativamente previsto dalla legge 241/1990, che può essere esperito solo in presenza di un interesse diretto, concreto e attuale, corrispondente a una situazione giuridicamente tutelata e collegata al documento al quale è chiesto l’accesso, deve essere accompagnato da una motivazione e si esercita con la visione e l’estrazione di copia dei documenti amministrativi²⁹. L’accesso civico è strumento distinto, dotato di diversa finalità, in quanto è preordinato a garantire la pubblicazione di documenti, informazioni e dati la cui pubblicazione è obbligatoria per legge, permettendo un controllo democratico sul rispetto delle norme³⁰.

Alla richiesta di accesso civico l’amministrazione è tenuta a provvedere entro trenta giorni e, in caso di ritardo o mancata risposta, si espone all’eventuale ricorso da parte del richiedente al titolare del potere sostitutivo o al giudice amministrativo³¹.

²⁶ Merita precisare che, seppur il decreto Trasparenza compia un riordino degli obblighi di pubblicazione, alcuni obblighi non sono compresi nel d.lgs. 33/2013, ma sono previsti da norme vigenti, precedenti e successive: per esempio gli obblighi di pubblicazione previsti in materia di *class action* dagli art. 1, comma 2, e art. 4, commi 2 e 6, d.lgs. 20 dicembre 2009, n. 198 e l’obbligo di pubblicazione da parte dei soggetti sperimentatori dei casi in cui il rilascio delle autorizzazioni di competenza è sostituito da una comunicazione dell’interessato in materia di zone a burocrazia zero, ai sensi di quanto previsto dall’art. 37, comma 3, d.l. 21 giugno 2013, n. 69 convertito con modificazioni dalla legge 9 agosto 2013, n. 98. Per un quadro maggiormente esaustivo degli obblighi di pubblicazione in capo alle amministrazioni cfr. la citata delibera CiVIT n. 50 del 4 luglio 2013, recante *Linee guida per l’aggiornamento del Programma triennale per la trasparenza e l’integrità 2014-2016* e relativi allegati.

²⁷ Art. 9, comma 1, del d.lgs. 33/2013, secondo cui le amministrazioni non possono disporre filtri e altre soluzioni tecniche atte ad impedire ai motori di ricerca *web* di indicizzare ed effettuare ricerche all’interno della sezione “Amministrazione trasparente”. L’allegato A del d.lgs. 33/2013 dettaglia struttura e organizzazione dei contenuti della sezione “Amministrazione Trasparente” dei siti *web* istituzionali.

²⁸ L’accesso civico è previsto all’art. 5 del d.lgs. 33/2013. La richiesta di accesso civico deve essere presentata al responsabile della trasparenza dell’amministrazione obbligata alla pubblicazione, che si pronuncia sulla stessa.

²⁹ Art. 22 e ss. della legge 241/1990.

³⁰ Sulle differenze relative ai due istituti si sofferma la citata circolare n. 2 del 19 luglio 2013 della Presidenza del Consiglio dei ministri – Dipartimento della Funzione Pubblica, *D.lgs. n. 33/2013 – Attuazione della trasparenza*, in <http://www.funzionepubblica.gov.it>.

³¹ In specifico l’amministrazione, entro trenta giorni, procede alla pubblicazione nel sito del documento, dell’informazione o del dato richiesto e lo trasmette contestualmente al richiedente ovvero comunica al medesimo l’avvenuta pubblicazione, indicando il collegamento ipertestuale a quanto richiesto. Se il documento, l’informazione o il dato richiesti risultano già pubblicati nel rispetto della normativa vigente, l’amministrazione deve indicare al

Il decreto Trasparenza, al fine di garantire effettività a quanto disposto, oltre all'introduzione dell'accesso civico, ha previsto strumenti di vigilanza sull'attuazione delle disposizioni e sanzioni relative al mancato rispetto delle norme³².

Pertanto si muniscono gli obblighi di pubblicazione della possibilità di eliminare aloni di opacità con il ricorso all'accesso civico, con la vigilanza sull'attuazione e con la sanzione di eventuali inadempimenti.

Nel percorso normativo recente, perciò, sono aumentati, sono stati fortificati e uniformati gli obblighi di pubblicazione delle amministrazioni, che dovranno riorganizzare i propri processi per garantire un'informazione completa, aggiornata e di qualità³³, preoccupandosi della pubblicazione fin dal momento della produzione del dato, nell'ottica di vere e proprie case di vetro virtuali³⁴, le cui funzioni e attività siano facilmente conoscibili dagli utenti.

3.2 Gli open data

La trasparenza, pertanto, si amplia e si affina nei suoi contenuti, si rafforza negli obblighi, diventa ordinata, effettiva, strutturata, ma non solo. La trasparenza matura anche nella sua natura, dal momento che, sotto stimolo dell'Unione europea³⁵, l'evoluzione normativa ha posto attenzione

richiedente il relativo collegamento ipertestuale (art. 5, comma 3, d.lgs. 33/2013). In caso di ritardo o mancata risposta, l'amministrazione si espone a eventuale ricorso da parte del richiedente al titolare del potere sostitutivo, di cui all'art. 2, comma 9-bis, legge 241/1990, che verificata la sussistenza dell'obbligo provvede, o al giudice amministrativo, ai sensi del d.lgs. 2 luglio 2010, n. 104 (art. 5, commi 4 e 5, d.lgs. 33/2013).

³² In particolare Capo VI (art. 43 e ss.) del d.lgs. 33/2013. La vigilanza sull'attuazione delle disposizioni viene affidata a una serie di soggetti interni ed esterni all'amministrazione, quali il Responsabile della trasparenza, gli Organismi Indipendenti di Valutazione (OIV) e la CiVIT, anche in qualità di Autorità Nazionale Anticorruzione (ANAC) (con il d.l. 31 agosto 2013, n. 101, convertito con modificazioni dalla legge 30 ottobre 2013, n. 125, la CiVIT, già individuata dalla legge 190/2012 quale Autorità nazionale anticorruzione, ha assunto la denominazione di Autorità Nazionale Anticorruzione e per la valutazione e la trasparenza delle amministrazioni pubbliche). L'inadempimento delle disposizioni comporta responsabilità dirigenziale, è eventuale causa di responsabilità per danno all'immagine dell'amministrazione e comporta comunque una valutazione ai fini della corresponsione della retribuzione di risultato e del trattamento accessorio collegato alla performance individuale dei responsabili (art. 46 d.lgs. 33/2013); sono previste inoltre sanzioni per casi specifici, quali sanzioni amministrative (art. 47 d.lgs. 33/2013), sanzioni che bloccano l'efficacia del provvedimento (art. 15, comma 2, e art. 26, comma 3, d.lgs. 33/2013), sanzioni consistenti nel mancato trasferimento di risorse a favore di enti e di organismi (artt. 22, comma 4, e 28, comma 2, d.lgs. 33/2013) e nell'obbligo di pubblicazione del provvedimento (art. 47 d.lgs. 33/2013). Le sanzioni riguardano non solo il responsabile della trasparenza per le sue attribuzioni e i suoi compiti, ma anche i dirigenti e gli organi politici tenuti a garantire il flusso delle informazioni di competenza, oggetto di pubblicazione (in tal senso la citata circolare n. 2 del 19 luglio 2013 della Presidenza del Consiglio dei ministri – Dipartimento della Funzione Pubblica, *D.lgs. n. 33/2013 – Attuazione della trasparenza*).

³³ Sulla qualità delle informazioni cfr. paragrafo 2.1.3.

³⁴ Sul concetto di "casa di vetro" P. DOMENICONI, F. SCARPIELLO, *La legge n. 15/2009: fra trasparenza ed eccesso di informazione*, in "Azienditalia – Il Personale", n. 5, 2009, pp. 227- 233, riferendosi alla metafora dell'on. Filippo Turati in Atti del Parlamento italiano, Camera dei deputati, sess. 1904-1908, 17 giugno 1908, p. 22962.

³⁵ Nel dicembre 2011 la Commissione europea ha presentato la strategia europea relativa al "pacchetto *open data*". Nella comunicazione ufficiale (*Dati aperti. Un motore per l'innovazione, la crescita e una governance trasparente*), finalizzata a valorizzare gli *open data* tra i Paesi europei, la Commissione ha lanciato una strategia composta da una serie di misure dirette allo scopo, quali l'adeguamento del quadro giuridico, investimenti finanziari dedicati, un portale europeo, un portale paneuropeo, ecc. In tale direzione è stata recentemente approvata con direttiva 2013/37/UE la revisione

crescente non solo alla quantità dei dati che devono essere pubblicati, quindi al *quantum*, ma anche al “come” dei dati, agli *open data*.

Pertanto recentemente le norme si interessano al *quomodo* della trasparenza. E’ complice anche la crisi finanziaria, che nella difficoltà di dare sostegno economico alle imprese porta a trovare soluzioni diverse e alternative per favorire la competitività: rientra sicuramente fra queste “dare i dati”, che formano la “miniera” del patrimonio informativo pubblico³⁶.

Il paradigma che emerge è quello di restituire i dati alla collettività per mezzo degli *open data*³⁷ e lasciare che l’intelligenza collettiva ne faccia uso, potendoli trasformare in leve di inedite potenzialità economiche e sociali. L’attenzione si concentra quindi nella possibilità di impiegare i dati per realizzare nuove analisi, servizi e soluzioni in grado di generare crescita economica e sociale. Inoltre gli *open data*, strumento di trasparenza ed elemento fondamentale dell’*open government*, permettono il controllo democratico dei cittadini, idoneo a garantire maggiore efficienza pubblica e ad allontanare tentativi di corruzione.

L’approccio di promozione esplicita degli *open data* è degli ultimissimi anni.

Infatti, nel d.lgs. 36/2006, che attua la direttiva 2003/98/CE (recentemente modificata dalla direttiva 2013/37/UE), non è imposto l’obbligo di consentire il riutilizzo dei documenti contenenti dati pubblici, che resta scelta dell’amministrazione, seppur i dati pubblici siano già visti come importante “materia prima” per prodotti e servizi digitali, da riutilizzare per contribuire alla crescita economica e sociale.

È necessario arrivare al 2010 per un’ottica di maggior incentivo con l’inserimento del comma 1-bis nell’art. 52 del d.lgs. 82/2005 da parte del d.lgs. 235/2010 (articolo ora modificato dal decreto Crescita 2.0), che può già essere interpretato come invito alle amministrazioni a promuovere *open data*³⁸. Poi, con l’art. 47 del c.d. decreto Semplificazioni, il legislatore assume maggiore coraggio e si

della direttiva europea sul riutilizzo dell’informazione del settore pubblico, direttiva 2003/98/CE, recepita in Italia con il d.lgs. 36/2006.

³⁶ Sugli *open data* cfr. T. AGNOLONI, M.T. SAGRI, D. TISCORNIA, *Open data: nuova frontiera della libertà informatica?*, in “Informatica e diritto”, n. 2, 2009, pp. 7-19. Sul valore e i vantaggi dei dati aperti cfr. M.C. DE VIVO, A. POLZONETTI, P. TAPANELLI, *Open data, Business Intelligence e Governance nella Pubblica Amministrazione*, in D. TISCORNIA (a cura di), *Open data e riuso dei dati pubblici*, cit., pp. 239-262 e F. MARZANO *La trasparenza nella Pubblica Amministrazione passa dall’Open Data o l’Open Data passa dalla trasparenza?*, in D. TISCORNIA (a cura di), *Open data e riuso dei dati pubblici*, cit., pp. 287-303.

³⁷ I dati di tipo aperto (*open data*), ai sensi dell’art. 68, comma 3, lett. b), del d.lgs. 82/2005, modificato dal d.l. 179/2012 convertito con modificazioni dalla legge 221/2012, sono i dati che presentano le seguenti caratteristiche: 1) sono disponibili secondo i termini di una licenza che ne permetta l’utilizzo da parte di chiunque, anche per finalità commerciali, in formato disaggregato (dimensione giuridica); 2) sono accessibili attraverso le tecnologie dell’informazione e della comunicazione (ICT), ivi comprese le reti telematiche pubbliche e private, in formati aperti, sono adatti all’utilizzo automatico da parte di programmi per elaboratori e sono provvisti dei relativi metadati (dimensione tecnologica); 3) sono resi disponibili gratuitamente attraverso le ICT, ivi comprese le reti telematiche pubbliche e private, oppure sono resi disponibili ai costi marginali sostenuti per la loro riproduzione e divulgazione (dimensione economica). Per quanto attiene ai dati di tipo aperto prodotti dalle pubbliche amministrazioni si parla più specificatamente di *open government data*. Sugli *open government data* cfr. F. DI DONATO, *Lo stato trasparente. Linked open data e cittadinanza attiva*, cit.

³⁸ Il testo del comma 1-bis dell’art. 52 del CAD (ora superato dalle modifiche del d.l. 179/2012 convertito con modificazioni dalla legge 221/2012) prevedeva: “Le pubbliche amministrazioni, al fine di valorizzare e rendere fruibili i dati pubblici di cui sono titolari, promuovono progetti di elaborazione e di diffusione degli stessi anche attraverso l’uso di strumenti di finanza di progetto, assicurando: a) il rispetto di quanto previsto dall’articolo 54, comma 3 [ossia fruibilità in rete gratuita senza necessità di identificazione informatica]; b) la pubblicazione dei dati e dei documenti in formati aperti di cui all’articolo 68, commi 3 e 4”.

spinge a inserire fra gli obiettivi della cabina di regia per l'attuazione dell'Agenda digitale italiana la “promozione del paradigma dei dati aperti (*open data*) quale modello di valorizzazione del patrimonio informativo pubblico, al fine di creare strumenti e servizi innovativi”³⁹.

Successivamente, con l'art. 18 del d.l. 83/2012 convertito con modificazioni dalla legge 134/2012, rubricato significativamente “Amministrazione aperta” (ora abrogato e confluito nei suoi contenuti nel cosiddetto decreto Trasparenza, d.lgs. 33/2013), si dispone la pubblicazione in formato aperto di determinate tipologie di informazioni, particolarmente rilevanti, quali in specifico la concessione di sovvenzioni, contributi, sussidi e ausili finanziari alle imprese e l'attribuzione dei corrispettivi e dei compensi a persone, professionisti, imprese ed enti privati e comunque di vantaggi economici di qualunque genere di cui all'art. 12 della legge 241/1990 ad enti pubblici e privati⁴⁰.

La norma, oltre a porre l'obbligo dal 1° gennaio 2013, prevede specifiche responsabilità e sanzioni in caso di inosservanza: da quella data, la pubblicazione costituisce condizione legale di efficacia del titolo legittimante delle concessioni e attribuzioni di importo superiore a mille euro, che è rilevata d'ufficio dagli organi dirigenziali e di controllo sotto la propria diretta responsabilità amministrativa, patrimoniale e contabile per l'indebita concessione o attribuzione del beneficio economico, ma è altresì rilevabile dal destinatario della concessione o attribuzione e da chiunque altro abbia interesse, anche ai fini del risarcimento del danno da ritardo.

Si tratta quindi di una norma molto importante sia per la tipologia dei dati aperti, sia per la forza delle disposizioni e delle conseguenze sanzionatorie.

Di recente, il cosiddetto decreto Crescita 2.0, il d.l. 179/2012 convertito con modificazioni dalla legge 221/2012, con l'art. 9, attraverso modifiche e integrazioni del CAD (artt. 52 e 68), ha introdotto la definizione espressa e opportuna di *open data* nelle dimensioni tecnologica, giuridica ed economica⁴¹ e ha inserito una norma generale con la finalità di razionalizzare il processo di valorizzazione del patrimonio informativo pubblico nazionale.

In specifico l'art. 52 del CAD, come modificato e integrato, prevede che l'accesso telematico a dati, documenti e procedimenti e il riutilizzo dei dati e documenti siano disciplinati dalle pubbliche amministrazioni⁴², obbligate a pubblicare sul proprio sito *web* il catalogo dei dati, dei metadati e delle relative banche dati in loro possesso e i regolamenti che ne disciplinano l'esercizio della facoltà di accesso telematico e il riutilizzo, fatti salvi i dati presenti in Anagrafe tributaria⁴³.

³⁹ Art. 47, comma 2-bis, lett. b), d.l. 5/2012 convertito con modificazioni dalla legge 35/2012.

⁴⁰ Ai sensi della norma in oggetto, i dati devono essere resi di facile consultazione, accessibili ai motori di ricerca e in formato tabellare aperto che ne consenta l'esportazione, il trattamento e il riuso.

⁴¹ Cfr. nota 37. Inoltre viene inserita la definizione di “formato dei dati di tipo aperto”, ossia un formato di dati reso pubblico, documentato esaurientemente e neutro rispetto agli strumenti tecnologici necessari per la fruizione dei dati stessi (art. 68, comma 3, lett. a), sostituito dall'art. 9 del d.l. 179/2012 convertito con modificazioni dalla legge 221/2012) e viene introdotta la definizione di “riutilizzo” come uso del dato di cui all'art. 2, comma 1, lett. e), del d.lgs 36/2006, ossia l'uso del dato di cui è titolare una pubblica amministrazione o un organismo di diritto pubblico, da parte di persone fisiche o giuridiche, a fini commerciali o non commerciali diversi dallo scopo iniziale per il quale il documento che lo rappresenta è stato prodotto nell'ambito dei fini istituzionali (art. 1, comma 1, lett. n-bis), d.lgs. 82/2005 inserita dall'art. 9 d.l. 179/2012 convertito con modificazioni dalla legge 221/2012).

⁴² L'obbligo riguarda tutti i soggetti cui si applica il codice dell'amministrazione digitale previsti dall'art. 2, comma 2, d.lgs. 82/2005.

⁴³ Art. 52, comma 1, d.lgs. 82/2005 come modificato, da ultimo, dal d.l. 179/2012 convertito con modificazioni dalla legge 221/2012.

La norma pone il principio dell'“*open data by default*”⁴⁴: i dati e i documenti pubblicati dalle amministrazioni con qualsiasi modalità, senza l'espressa adozione di una licenza, si intendono rilasciati come dati di tipo aperto. L'eventuale adozione di una licenza⁴⁵ deve essere motivata ai sensi delle linee guida nazionali definite dall'Agenzia per l'Italia digitale⁴⁶.

Le pubbliche amministrazioni, inoltre, nella definizione dei capitolati o degli schemi dei contratti di appalto relativi a prodotti e servizi che comportino la raccolta e la gestione di dati pubblici, sono tenute a prevedere clausole idonee a consentire l'accesso telematico e il riutilizzo, da parte di persone fisiche e giuridiche, di tali dati, dei metadati, degli schemi delle strutture di dati e delle relative banche dati⁴⁷.

Al fine di assicurare effettività a quanto previsto, l'art. 52 del CAD collega espressamente le attività volte a garantire l'accesso telematico e il riutilizzo dei dati delle pubbliche amministrazioni ai parametri di valutazione della performance dirigenziale⁴⁸.

Si delinea pertanto un chiaro *favor* del legislatore verso gli *open data* in considerazione delle finalità che permettono di realizzare, quali trasparenza, sviluppo personale e sociale dei cittadini e possibilità di crescita economica per le imprese.

In materia di valorizzazione del patrimonio informativo pubblico, la disposizione assegna un ruolo centrale a livello nazionale all'Agenzia per l'Italia digitale⁴⁹, individuata come organismo designato a vigilare sulla corretta attuazione delle disposizioni.

L'Agenzia è deputata a promuovere le politiche di valorizzazione del patrimonio informativo pubblico nazionale e attuare le disposizioni del capo V del CAD. A tal fine, le sono assegnati specifici compiti con cadenza annuale: entro il mese di febbraio di ogni anno deve trasmettere al Presidente del Consiglio o al Ministro delegato per l'innovazione tecnologica, che li approva entro il mese successivo, l'Agenda nazionale in cui definisce contenuti e obiettivi delle politiche di valorizzazione del patrimonio informativo pubblico e un rapporto annuale sullo stato del processo di valorizzazione nel Paese⁵⁰.

⁴⁴ Parla di *open data by default* lo stesso portale governativo Dati.gov al link <http://www.dati.gov.it/content/parte-lopen-data-default> (comunicazione del 19 marzo 2013).

⁴⁵ La norma si riferisce all'art. 2, comma 1, lettera h), d.lgs. 36/2006, che definisce quale “licenza standard per il riutilizzo” il contratto, o altro strumento negoziale, redatto ove possibile in forma elettronica, nel quale sono definite le modalità di riutilizzo dei documenti delle pubbliche amministrazioni o degli organismi di diritto pubblico.

⁴⁶ Art. 52, comma 2, d.lgs. 82/2005 come modificato, da ultimo, dal d.l. 179/2012 convertito con modificazioni dalla legge 221/2012. Le *Linee guida nazionali per la valorizzazione del patrimonio informativo pubblico (secondo semestre 2013)* sono state approvate nella versione 1.0 dall'Agenzia per l'Italia digitale il 31 luglio 2013.

⁴⁷ Art. 52, comma 3, d.lgs. 82/2005 come modificato, da ultimo, dal d.l. 179/2012 convertito con modificazioni dalla legge 221/2012.

⁴⁸ Art. 52, comma 4, d.lgs. 82/2005 come modificato, da ultimo, dal d.l. 179/2012 convertito con modificazioni dalla legge 221/2012.

⁴⁹ L'Agenzia per l'Italia digitale – AgID è stata istituita a seguito degli artt. 19-22 del d.l. 83/2012 convertito con modificazioni dalla legge 134/2012 ed è andata a sostituire DigitPA, che a sua volta, a causa del riordino avvenuto con d.lgs. 1° dicembre 2009, n. 177, ha sostituito il Centro nazionale per l'informatica nella pubblica amministrazione – CNIPA (che aveva sostituito grazie all'art. 176 del d.lgs. 30 giugno 2003, n. 196 l'Autorità per l'informatica nella pubblica amministrazione – AIPA, istituita inizialmente con d.lgs. 12 febbraio 1993, n. 39).

⁵⁰ Art. 52, commi 5 e 6, d.lgs. 82/2005 come modificato, da ultimo, dal d.l. 179/2012 convertito con modificazioni dalla legge 221/2012. Il rapporto annuale è pubblicato in formato aperto sul sito istituzionale della Presidenza del Consiglio.

Date le proprie competenze istituzionali, accanto alle funzioni strategiche all’Agenzia è riservato anche un ruolo tecnico in materia, in quanto si prevede definisca e aggiorni annualmente le linee guida nazionali che individuano gli standard tecnici, compresa la determinazione delle ontologie dei servizi e dei dati, le procedure e le modalità di attuazione delle disposizioni con l’obiettivo di rendere il processo omogeneo a livello nazionale, efficiente ed efficace. Le pubbliche amministrazioni devono uniformarsi alle suddette linee guida⁵¹.

L’Agenzia per l’Italia digitale quindi è individuata come il soggetto deputato a “traghettare” le amministrazioni italiane verso l’apertura dei propri dati per mezzo di funzioni strategiche e tecniche a ciò finalizzate⁵².

In questo percorso normativo si inserisce oggi il d.lgs. 33/2013 (in cui sono confluite alcune delle norme esaminate, quali l’art. 18 del d.l. 83/2012 convertito con modificazioni dalla legge 134/2012⁵³), che statuisce nel suo art. 7, significativamente rubricato “*dati aperti e riutilizzabili*” il principio secondo cui i documenti, le informazioni e i dati oggetto di pubblicazione obbligatoria devono essere pubblicati in formato aperto e devono essere riutilizzabili, senza ulteriori restrizioni diverse dall’obbligo di citare la fonte e di rispettarne l’integrità⁵⁴.

3.3 Qualità delle informazioni e inclusione digitale

La rilevanza e l’ampiezza conferite ai criteri di trasparenza e apertura hanno portato le disposizioni a dedicare particolare attenzione al profilo della qualità delle informazioni, aspetto specificatamente disciplinato dall’art. 6 del d.lgs. 33/2013.

Le pubbliche amministrazioni devono garantire la qualità delle informazioni riportate nei siti istituzionali nel rispetto degli obblighi di pubblicazione previsti, assicurandone l’integrità, il costante aggiornamento, la completezza, la tempestività, la semplicità di consultazione, la comprensibilità, l’omogeneità, la facile accessibilità, la conformità ai documenti originali in possesso dell’amministrazione, l’indicazione della loro provenienza e la riutilizzabilità⁵⁵.

Alla qualità delle informazioni, già valorizzata nell’art. 53 del CAD fra le caratteristiche che i siti istituzionali devono rispettare, viene quindi dedicata tale disposizione specifica nel decreto Trasparenza nella consapevolezza che la qualità delle informazioni è essenziale per garantire una reale ed

⁵¹ Art. 52, comma 7, d.lgs. 82/2005 come modificato, da ultimo, dal d.l. 179/2012 convertito con modificazioni dalla legge 221/2012. Le *Linee guida nazionali per la valorizzazione del patrimonio informativo pubblico (secondo semestre 2013)* sono state approvate nella versione 1.0 dall’Agenzia per l’Italia digitale il 31 luglio 2013.

⁵² Il Presidente del Consiglio o il Ministro delegato per l’innovazione tecnologica riferisce annualmente al Parlamento sullo stato di attuazione delle disposizioni dell’art. 52 CAD (art. 52, comma 8, d.lgs. 82/2005 come modificato, da ultimo, dal d.l. 179/2012 convertito con modificazioni dalla legge 221/2012).

⁵³ L’art. 18 del d.l. 83/2012, convertito con modificazioni dalla legge 134/2012, è stato abrogato dal d.lgs. 33/2013 e i suoi contenuti sono ora confluiti nel d.lgs. 33/2013 (in particolare negli articoli 26 e 27).

⁵⁴ In merito all’apertura, l’art. 7 del d.lgs. 33/2013 chiarisce che i documenti, le informazioni e i dati oggetto di pubblicazione obbligatoria, resi disponibili anche a seguito dell’accesso civico, sono pubblicati in formato di tipo aperto ai sensi dell’art. 68 CAD e sono riutilizzabili ai sensi d.lgs. 36/2006, del d.lgs. 82/2005, e del d.lgs. 196/2003, senza ulteriori restrizioni diverse dall’obbligo di citare la fonte e di rispettarne l’integrità.

⁵⁵ Art. 6, comma 1, d.lgs. 33/2013.

efficace trasparenza e permettere la piena comprensione delle informazioni rese.

Prevedendo e prevenendo possibili *escamotage* con cui giustificare mancate o incomplete attuazioni delle disposizioni normative, a fini di effettività, il decreto Trasparenza precisa che l'esigenza di assicurare adeguata qualità delle informazioni diffuse non può, in ogni caso, costituire motivo per l'omessa o ritardata pubblicazione dei dati, delle informazioni e dei documenti⁵⁶.

La trasparenza e l'apertura dei dati, accanto all'attenzione ai profili legati alla sicurezza⁵⁷ e alla necessità di una comunicazione efficace, si sono tradotte anche in una forte attenzione all'inclusione digitale.

Così l'art. 9 del d.l. 179/2012 convertito con modificazioni dalla legge 221/2012, al fine di assicurare il rispetto dei requisiti di accessibilità⁵⁸, obbliga le amministrazioni a pubblicare ogni anno nel sito *web* gli obiettivi di accessibilità per l'anno corrente, introduce la possibilità di segnalazione delle inadempienze da parte degli interessati e prevede responsabilità e sanzioni scaturenti dall'inosservanza delle disposizioni a carico dei dirigenti dell'amministrazione⁵⁹. Trasparenza e apertura, infatti, devono sposarsi con l'eguaglianza sostanziale e non devono trasformarsi in una possibile nuova forma di discriminazione nell'accesso al patrimonio informativo pubblico.

Pertanto nel quadro normativo vigente, i dati pubblici sono curati nella loro qualità e vengono aperti, in modo che possano essere riutilizzati da altre amministrazioni, cittadini e imprese, facendo emergere la fisionomia di un'amministrazione in cui l'*openness* è il metodo di svolgimento delle

⁵⁶ Art. 6, comma 2, d.lgs. 33/2013.

⁵⁷ Per i profili legati alla sicurezza cfr. G. PREITE, *Habeas data tra sicurezza e privacy: quale politica per i nuovi diritti?*, in M. SIRIMARCO (a cura di) "Info-ius. Problemi e prospettive dell'informatica giuridica", Roma, Nuova Cultura, 2010, pp. 279-304.

⁵⁸ L'art. 2, comma 1, lett. a), legge 9 gennaio 2004, n. 4, recante "Disposizioni per favorire l'accesso dei soggetti disabili agli strumenti informatici" (cosiddetta legge Stanca) definisce accessibilità "la capacità dei sistemi informatici, nelle forme e nei limiti consentiti dalle conoscenze tecnologiche, di erogare servizi e fornire informazioni fruibili, senza discriminazioni, anche da parte di coloro che a causa di disabilità necessitano di tecnologie assistive o configurazioni particolari". La legge chiarisce all'art. 2, comma 1, lett. b) che sono tecnologie assistive "gli strumenti e le soluzioni tecniche, *hardware* e *software*, che permettono alla persona disabile, superando o riducendo le condizioni di svantaggio, di accedere alle informazioni e ai servizi erogati dai sistemi informatici". Il tema dell'accessibilità è disciplinato dalla citata legge 4/2004, dal relativo d.p.r. 1° marzo 2005, n. 75 (regolamento di attuazione della legge 4/2004, che tratta i requisiti necessari per l'accessibilità e disciplina la valutazione dell'accessibilità) e dal conseguente d.m. 8 luglio 2005 (linee guida recanti i requisiti tecnici e i diversi livelli per l'accessibilità). Di inclusione digitale si è occupato poi l'art. 9 del d.l. 179/2012 convertito con modificazioni dalla legge 221/2012. Da ultimo, è stato approvato il decreto 20 marzo 2013, "Modifiche all'allegato A del decreto 8 luglio 2005 del Ministro per l'innovazione e le tecnologie, recante: «Requisiti tecnici e i diversi livelli per l'accessibilità agli strumenti informatici»" (in Gazzetta Ufficiale n. 217 del 16 settembre 2013) ed è stata emanata e pubblicata da parte dell'Agenzia per l'Italia digitale la circolare n. 61 del 29 marzo 2013 relativa agli obblighi di accessibilità per la PA, recante *Disposizioni del decreto legge 18 ottobre 2012, n. 179, convertito con modificazioni dalla L. 17 dicembre 2012, n. 221 in tema di accessibilità dei siti web e servizi informatici. Obblighi delle pubbliche Amministrazioni*, in <http://www.digitpa.gov.it>.

⁵⁹ Specificatamente, entro il 31 marzo di ogni anno, le pubbliche amministrazioni devono pubblicare nel proprio sito *web* gli obiettivi di accessibilità per l'anno corrente. A fini di effettività si introduce lo strumento della segnalazione; gli interessati che rilevino inadempienze in ordine all'accessibilità dei servizi erogati ne fanno formale segnalazione, anche in via telematica, all'Agenzia per l'Italia digitale. Qualora l'Agenzia ritenga la segnalazione fondata, richiede l'adeguamento dei servizi assegnando un termine non superiore a 90 giorni. In caso di inosservanza delle disposizioni sull'accessibilità (inclusa la mancata pubblicazione degli obiettivi) sono specificate le responsabilità conseguenti che consistono nella rilevanza ai fini della misurazione e della valutazione della performance individuale dei dirigenti responsabili e nella responsabilità dirigenziale e disciplinare, ferme restando le eventuali responsabilità penali e civili previste dalle disposizioni vigenti (art. 9, commi 7 e seguenti, d.l. 179/2012 convertito con modificazioni dalla legge 221/2012).

proprie funzioni. L'apertura si traduce anche nell'inclusione digitale, al fine di garantire parità di accesso all'informazione e rispetto del principio costituzionale di eguaglianza sostanziale.

I dati pubblici di tipo aperto agiscono come strumenti di trasparenza, ma al tempo stesso anche di partecipazione e collaborazione, permettendo agli utenti di generare prodotti e servizi che possono rivelarsi utili alle stesse amministrazioni, attivando un circolo virtuoso alimentato dall'intelligenza collettiva.

Oltre agli *open data*, il principio di partecipazione si traduce in una serie di ulteriori strumenti previsti e incentivati dalle norme recenti.

4 Partecipazione

4.1 Servizi in rete e customer satisfaction

Il principio di partecipazione consente a cittadini e imprese di svolgere un ruolo attivo e di essere coinvolti nelle attività delle amministrazioni pubbliche. Il principio trova forma nell'apertura dei servizi al fine di costruirli insieme e per gli utenti, utilizzando il loro apporto al momento della progettazione, durante lo svolgimento e dopo l'erogazione.

Anche da questo punto di vista le norme offrono riferimenti importanti.

L'attenzione all'utente e alla *customer satisfaction* è prevista dalle norme del CAD, in particolare dagli articoli 7 e 63, come in seguito modificati⁶⁰.

Le amministrazioni, nella reingegnerizzazione e nell'aggiornamento dei servizi resi, devono costruire un rapporto costante con gli utenti nella progettazione del servizio (*ex ante*), durante la sua erogazione e successivamente (*ex post*), permettendo un *feedback* durante tutto il "ciclo di vita" del servizio, grazie all'adozione di strumenti, come quelli del *web 2.0*, idonei alla rilevazione immediata, continua e sicura del giudizio degli utenti.

Risulta pertanto determinante analizzare e interpretare correttamente le reali esigenze dei cittadini e delle imprese e valutare il grado di soddisfazione dell'utenza nello svolgimento delle funzioni e nell'erogazione dei servizi, al fine di sviluppare un'amministrazione pubblica realmente aperta alle istanze della collettività e alla realizzazione del suo benessere. Infatti, cittadini e imprese, quali utilizzatori dei servizi, li conoscono in modo puntuale e sono in grado di rilevare criticità, suggerire modifiche e integrazioni, collaborare a miglioramenti. Gli strumenti di *customer satisfaction* consentono quindi agli utenti di partecipare alle azioni e alle funzioni pubbliche, agendo un costante controllo e innescando una proficua collaborazione, al fine di realizzare servizi migliori⁶¹.

L'ottica dei servizi *online* risulta molto favorita nella normativa recente, in particolare dal d.l. 5/2012 convertito con modificazioni dalla legge 35/2012, divenendo via obbligata per le amministrazioni

⁶⁰ In particolare le modifiche si sono avute con il d.lgs. 235/2010 e con il d.l. 5/2012 convertito con modificazioni dalla legge 35/2012.

⁶¹ Sulla *customer satisfaction* cfr. C. GIANFELICI, *Le indagini di customer satisfaction nelle amministrazioni pubbliche: finalità, metodologia e strumenti*, in "Azienditalia", n. 1, 2009, pp. 1-29.

dal 1° gennaio 2014. Da questa data le amministrazioni dovranno utilizzare esclusivamente canali e servizi telematici per la presentazione di denunce e istanze, per l'esecuzione di versamenti, per la richiesta di attestazioni e certificazioni, per gli atti, le comunicazioni e i servizi resi⁶². Si passa così dall'obbligatorietà del servizio a una sorta di obbligatorietà della sua erogazione *online*, divenendo la modalità digitale la regola dell'azione pubblica⁶³.

I servizi *online*, come si è visto, dovranno essere progettati e aggiornati servendosi di strumenti di contatto e di rilevazione del *feedback* di cittadini e imprese, in modo da realizzare un rapporto costante con gli utenti e permettere così un'azione pubblica efficace ed efficiente, idonea a rispondere alle esigenze reali espresse dalla collettività.

4.2 E-democracy

Le tecnologie, inoltre, accanto al proficuo utilizzo nello svolgimento delle funzioni e nell'erogazione dei servizi, possono essere implementate anche per assicurare il coinvolgimento nei processi decisionali, per permettere il controllo democratico e per facilitare iniziative dirette dei cittadini. Pertanto le nuove tecnologie possono essere utilizzate per dare sostanza all'*e-democracy*, prevista e incentivata dalle norme, in particolare dall'art. 9 del CAD⁶⁴.

La democrazia elettronica può trovare forma in diversi strumenti, quali la pubblicazione di informazioni e documentazione sul *web*, *newsletter*, *forum*, sondaggi, le consultazioni pubbliche *online*, il voto elettronico.

Gli strumenti di democrazia elettronica permettono di rendere aperte le azioni dei governi e delle amministrazioni nella logica dell'*open government*, garantendo trasparenza e coinvolgimento nei processi decisionali per mezzo della raccolta di osservazioni e *feedback*, provocando così un avvicinamento dei cittadini, idoneo a sanare la distanza dai decisori.

Si configura come preconditione dei processi di *e-democracy* il contrasto al *digital divide*⁶⁵ e la conseguente inclusione digitale, necessari a garantire parità nel coinvolgimento ed effettiva eguaglianza

⁶² Art. 63, comma 3-bis e ss., d.lgs. 82/2005, come modificato dal d.l. 5/2012 convertito con modificazioni dalla legge 35/2012. E' rimessa a un decreto del Presidente del Consiglio dei Ministri l'individuazione di deroghe ed eventuali limitazioni al principio di esclusività. A queste previsioni le norme accompagnano l'obbligo di pubblicazione sul sito *web* dell'elenco dei provvedimenti adottati, dei termini e delle modalità di utilizzo dei servizi, dei canali telematici e della posta elettronica certificata.

⁶³ L'evoluzione verso una sorta di obbligatorietà dell'erogazione *online* dei servizi si nota già nella profonda riforma apportata dal d.lgs. 235/2010 al d.lgs. 82/2005. In merito cfr. F. FAINI, *Dati, siti e servizi in rete delle pubbliche amministrazioni: l'evoluzione nel segno della trasparenza del decreto legislativo n. 235 del 2010*, cit., pp. 263-286.

⁶⁴ Il d.lgs. 82/2005 prevede espressamente la partecipazione democratica elettronica all'art. 9: "Le pubbliche amministrazioni favoriscono 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".

⁶⁵ Si intende per *digital divide* il divario tra chi accede, fruisce e utilizza le tecnologie dell'informazione e della comunicazione e chi ne è escluso, in modo parziale o totale. Sono diverse le motivazioni di esclusione: geografiche e infrastrutturali, culturali, anagrafiche, economiche, inerenti a disabilità. In merito cfr. P. TARALLO (a cura di), A. BUONGIOVANNI, F. MARZANO, E. TESI, P. ZECCHI, *Digital divide. La nuova frontiera dello sviluppo globale*, Milano, Franco Angeli, 2003.

tra i cittadini⁶⁶. Sono processi che pertanto dovranno essere accompagnati da interventi in tal senso, oltre che da azioni che permettano effettiva trasparenza e comunicazione efficace degli strumenti utilizzati, per garantirne la piena comprensione⁶⁷.

Tutto questo presuppone un nuovo modo di relazionarsi fondato sulla partecipazione immediata e continua da parte di cittadini e imprese che miri alla condivisione delle scelte, insieme alla co-progettazione e co-gestione dei servizi, che richiamano un altro principio fondamentale dell'*open government*, la collaborazione.

5 Collaborazione

5.1 Cloud computing, riuso e open source

Il principio di collaborazione si riconosce nell'insieme integrato di alcuni strumenti previsti e favoriti dalla normativa recente, che permettono un'azione sinergica e maggiormente uniforme da parte delle amministrazioni pubbliche: *cloud computing*, riuso e *software* libero.

La logica del sistema pubblico omogeneo e collaborativo trova linfa nel *cloud computing*⁶⁸, che promuove un approccio unitario, comportando razionalizzazione, permettendo risparmi economici e agendo da moltiplicatore degli investimenti.

Il *cloud computing* lascia al passato la logica dei sistemi che si moltiplicano nel “fai da te” delle diverse amministrazioni, anche le più piccole, logica che costa al sistema pubblico e finisce spesso per non essere funzionale. La condivisione dei sistemi stimola maggiore collaborazione fra gli enti coinvolti anche sotto il profilo strategico e progettuale, esattamente nella logica che ispira il governo

⁶⁶ In tal senso M. TEDESCHI, *E-Democracy*, in DE PIETRO L. (a cura di), *Dieci lezioni per capire ed attuare l'e-government*, Venezia, Marsilio editori, 2011, p. 155 e ss., che sottolinea quali precondizioni di *e-democracy* l'inclusione sociale e l'*e-government*.

⁶⁷ In merito all'*e-democracy* solleva alcuni profili di criticità e contraddizione M. CUNIBERTI (a cura di), *Nuove tecnologie e libertà della comunicazione. Profili costituzionali e pubblicistici*, nella collana FRANCESCHELLI V., TOSI E. (a cura di), *Diritto delle nuove tecnologie*, Milano, Giuffrè, 2008, pp. 358-359, secondo cui “mentre si coltiva il mito del procedimento il più possibile partecipato e aperto, anche attraverso le forme della c.d. *e-participation*, svanisce e si affievolisce l'idea e la sostanza della responsabilità politica: un'amministrazione che ascolta tutti, un'amministrazione “oggettivata”, che in fondo non fa scelte ma si limita a dare spazio alle istanze provenienti dalla società, è un'amministrazione che non può neppure essere discussa, né può essere chiamata a rispondere di scelte che, in fin dei conti, non appaiono neppure come sue”.

⁶⁸ Il *cloud computing* (nuvola informatica) secondo la definizione ufficiale che ne dà al riguardo il NIST (*National Institute of Standards and Technology*) è un “modello per abilitare un accesso di rete conveniente e su richiesta a un insieme condiviso di risorse computazionali configurabili (per esempio reti, server, memoria di massa, applicazioni e servizi), che possono essere rapidamente procurate e rilasciate con un minimo sforzo di gestione o una limitata interazione con il fornitore di servizi”(trad. it.). Il NIST associa alla definizione 5 caratteristiche essenziali (*on demand self service, broad network access, resource pooling, rapid elasticity, measured service*), 3 modelli di servizio (*SaaS – Software as a Service, PaaS – Platform as a Service e IaaS – Infrastructure as a Service*) e 4 modelli di distribuzione (*private cloud, community cloud, public cloud, hybrid cloud*). In merito cfr. R. RAZZANTE, *Manuale di diritto dell'informazione e della comunicazione. Privacy, diffamazione e tutela della persona. Libertà e regole nella Rete*, 5° ed., Padova, Cedam, 2011, p. 419, che con l'espressione *cloud computing* fa riferimento a “quell'insieme di tecnologie informatiche che consentono l'impiego di risorse *hardware* o *software* distribuite in remoto”.

aperto⁶⁹. Il *cloud computing* si configura quindi quale strumento per realizzare e favorire l'apertura e la collaborazione tra amministrazioni pubbliche e si pone come traduzione operativa di una logica "orizzontale" e non "verticale" (e verticistica) dell'azione delle diverse istituzioni.

Il *cloud computing* trova riconoscimento e stimolo nelle previsioni normative recenti. Così l'art. 47 del c.d. decreto Semplificazioni (d.l. 5/2012 convertito con modificazioni dalla legge 35/2012) significativamente pone fra gli obiettivi della cabina di regia per l'attuazione dell'Agenda digitale italiana "la promozione della diffusione e del controllo di architetture *cloud computing* per le attività e i servizi delle pubbliche amministrazioni"⁷⁰.

Il riconoscimento normativo non si arresta alla promozione del *cloud*. L'art. 9-bis del d.l. 179/2012 inserito dalla legge 221/2012, attraverso la modifica dell'art. 68, comma 1, del CAD, ha introdotto espressamente la fruibilità di *software* in modalità *cloud computing* fra le possibilità di acquisizione di programmi informatici da parte delle amministrazioni, a seguito della valutazione comparativa di tipo tecnico ed economico, accanto alle altre soluzioni previste, ossia lo sviluppo del *software* per conto dell'amministrazione, il riuso, l'acquisizione di *software* libero o l'acquisizione di *software* proprietario. Il *cloud computing* non è quindi solo incentivato, ma approda in modo riconosciuto nella realtà operativa delle istituzioni.

Riguardo allo sviluppo e all'acquisizione del *software*, nelle norme recenti sono poi fortificati due strumenti già presenti, ma senza la *vis* che è conferita loro oggi: si tratta del riuso e del *software* libero. Il principio di una pubblica amministrazione collaborativa trova strumento nel riuso dei sistemi e delle soluzioni, che traduce la necessità di scambio di buone pratiche, in una sana competizione a utilizzare quanto fatto da altre amministrazioni, contribuendo a dare volto uniforme al sistema pubblico. Il riuso, che agisce come forte moltiplicatore di investimenti, permette risparmi di scala e uniformità nell'azione delle diverse amministrazioni. Presuppone e promuove l'agire collaborativo, essenziale al fine di poter conoscere e riutilizzare le soluzioni di altre amministrazioni.

Il riuso era già regolato dall'art. 69 del CAD in modo incisivo, prevedendo l'obbligo per le amministrazioni titolari di programmi informatici realizzati su specifiche indicazioni del committente pubblico di darli in formato sorgente in uso gratuito ad altre amministrazioni che li richiedono e che intendano adattarli alle proprie esigenze, salvo motivate ragioni.

Negli interventi normativi recenti, in aggiunta a questo, il riuso cessa di essere una delle possibili soluzioni e assurge a essere una fra le soluzioni preferenziali nell'acquisizione di *software*: è possibile, infatti, l'acquisizione di programmi di tipo proprietario mediante ricorso a licenza d'uso, solo ove dalla valutazione comparativa di tipo tecnico ed economico risulti motivatamente l'impossibilità di accedere a soluzioni già disponibili all'interno della pubblica amministrazione o a *software* liberi o a codice sorgente aperto, adeguati alle esigenze da soddisfare⁷¹.

Le norme quindi favoriscono il ricorso al riuso, una delle soluzioni che prediligono insieme all'acquisizione di *software* libero. Scelta normativa anch'essa in linea con le esigenze di collaborazione e omogeneità, che comportano la necessità di sistemi flessibili e sostenibili, atti a ottimizzare le risorse e idonei a essere riutilizzati.

⁶⁹ In tal senso cfr. DigitPA (oggi Agenzia per l'Italia digitale), *Raccomandazioni e proposte sull'utilizzo del cloud computing nella pubblica amministrazione*, versione 2.0, 28 giugno 2012, in <http://www.digitpa.gov.it>.

⁷⁰ Art. 47, comma 2-bis, lett. d) , d.l. 5/2012 convertito con modificazioni dalla legge 35/2012.

⁷¹ Così art. 68, comma 1-ter, d.lgs. 82/2005.

Per questo le norme recenti promuovono l'utilizzo di *software* libero o *open source*⁷², maggiormente idoneo a realizzare tali obiettivi e atto peraltro a promuovere pluralismo e crescita della competitività. Prima il d.l. 83/2012, convertito con modificazioni dalla legge 134/2012, e ora l'art. 9-bis del d.l. 179/2012, convertito con modificazioni dalla legge 221/2012, hanno abbracciato questa prospettiva favorevole, oltre che al riuso, all'*open source*⁷³ prevedendo, come visto, che l'acquisizione di *software* libero o a codice sorgente aperto o il ricorso a soluzioni già sviluppate siano la regola generale e confinando l'acquisizione di *software* di tipo proprietario a ipotesi residuale, consentita solo a determinate condizioni. Il virtuoso "combinato disposto" costituito da *cloud computing*, riuso e *open source* caratterizza quindi normativamente l'amministrazione digitale aperta per quanto attiene al funzionamento del sistema pubblico, dando forma concreta al principio di collaborazione, pilastro del modello di *open government*.

5.2 Il web 2.0 e le smart communities

Il principio di collaborazione, oltre che all'interno del mondo pubblico, si sostanzia anche in strumenti che permettono la co-progettazione e la co-gestione dei servizi con utenti esterni (cittadini, associazioni e imprese). Da questo punto di vista sicuramente l'utilizzo di strumenti del *web 2.0* nell'erogazione dei servizi stimola una maggiore partecipazione e una co-produzione nella logica dell'*user-generated content*⁷⁴.

Gli strumenti del *web 2.0* costituiscono mezzi concreti per assicurare la collaborazione di cittadini e imprese all'azione pubblica, garantire una correlata maggiore efficienza alle amministrazioni e permettere di valutare il miglioramento della qualità della vita e il correlato benessere della collettività; possono ritenersi favoriti dalle norme che prevedono il diritto all'uso delle tecnologie, la qualità dei servizi resi, la soddisfazione dell'utenza e la democrazia elettronica⁷⁵. La normativa, come visto⁷⁶, favorisce i servizi *online* e dispone di analizzare le reali esigenze degli utenti e valutarne il grado di soddisfazione nello svolgimento delle funzioni e nell'erogazione dei servizi, al fine di dare vita a un'amministrazione pubblica aperta all'apporto collaborativo della collettività.

⁷² Nel *software open source*, l'uso è concesso con una licenza che conferisce la libertà di eseguire, studiare, adattare, modificare, migliorare, distribuire il *software*: è reso disponibile il codice sorgente (a differenza del *software closed source*). Su *software open source* e *software* proprietario cfr. G. SARTOR, *L'informatica giuridica e le tecnologie dell'informazione – Corso d'informatica giuridica*, cit., p. 122 e seguenti.

⁷³ Le norme citate hanno modificato il CAD (in specifico il suo art. 68).

⁷⁴ L'evoluzione in senso partecipativo di Internet ha visto il passaggio dal *web 1.0*, caratterizzato da siti statici e servizi offerti in maniera unilaterale senza interazione dell'utente (tranne navigazione, *mail* e motori di ricerca), al *web 2.0*, caratterizzato da una serie di applicazioni e servizi che garantiscono un alto livello di interazione sito-utente e si avvalgono in maniera sostanziale dei contributi degli utenti. Il *web* diventa testo "riscrivibile", in cui tutti possono partecipare alla sua evoluzione. Tipici strumenti del *web 2.0* sono i *social network site* (*Facebook*, *Twitter*, *LinkedIn*), le piattaforme per la condivisione di contenuti (*YouTube*, *Flickr*), *blog*, *wiki* (*Wikipedia*), ecc. In tal senso e per un'analisi del *web 2.0* cfr. G. SARTOR, *L'informatica giuridica e le tecnologie dell'informazione – Corso d'informatica giuridica*, cit., p. 236 e seguenti.

⁷⁵ Artt. 3, 7 e 9 del d.lgs. 82/2005. In tal senso E. BELISARIO, *La nuova Pubblica Amministrazione Digitale*, cit., p. 87 e seguenti.

⁷⁶ Cfr. paragrafo 2.2.1.

Nel nuovo quadro normativo di riferimento, la logica di partecipazione e collaborazione che trova forma negli strumenti esaminati, arriva a plasmare la stessa comunità di riferimento: si parla di *smart communities* o comunità intelligenti o, ancora, *smart cities*, cui la normativa recente ha prestato particolare attenzione.

L'art. 47 del d.l. 5/2012 convertito con modificazioni dalla legge 35/2012 pone, infatti, quale obiettivo specifico della cabina di regia per l'attuazione dell'Agenda digitale italiana la realizzazione delle infrastrutture tecnologiche e immateriali a servizio delle "comunità intelligenti" (*smart communities*), finalizzate a soddisfare la crescente domanda di servizi digitali in settori quali la mobilità, il risparmio energetico, il sistema educativo, la sicurezza, la sanità, i servizi sociali e la cultura⁷⁷.

Le norme non forniscono una vera e propria definizione di *smart community*, presente in altri atti e documenti pubblici, che la individuano in quel contesto territoriale, in cui l'utilizzo pianificato delle risorse umane e naturali, gestite e integrate mediante le ICT (*Information and Communication Technologies*), permette di affrontare congiuntamente tematiche riferibili alle sfide sociali emergenti (mobilità, ambiente, energia, qualità edilizia, sicurezza, ecc.), utilizzando al meglio le risorse e fornendo servizi integrati e "intelligenti"⁷⁸.

Le *smart communities* esprimono l'essenza e la funzione stessa che le tecnologie devono avere all'interno della società, ossia rendere più funzionale, più efficiente e più semplice la vita della collettività. Nel concetto di *smart city*, pertanto, le tecnologie non sono il fine, ma il mezzo preordinato all'obiettivo finale costituito dal benessere della collettività: lo sviluppo delle *smart cities* è collegato strettamente ai benefici apportati alla comunità di riferimento in termini di miglioramento della qualità della vita, creazione di occupazione, urbanizzazione sostenibile, sviluppo e risparmio economico⁷⁹.

Smart community significa pertanto innovazione non solo tecnologica, ma culturale, organizzativa, sociale, in ordine a competenze, ad attrazione di investimenti e a capacità di *governance*: tutto ciò presuppone l'inclusione, la partecipazione e la collaborazione della comunità, in una logica di

⁷⁷ Art. 47, comma 2-bis, lett. a) , d.l. 5/2012 convertito con modificazioni dalla legge 35/2012.

⁷⁸ Nell'*Avviso per la presentazione di idee progettuali per Smart Cities and Communities and Social Innovation* pubblicato dal MIUR - Ministero dell'Istruzione, dell'Università e della Ricerca - (si tratta del decreto direttoriale n. 391/Ric. del 5 luglio 2012) si dice che "la *Smart Community*, quale riferimento per l'individuazione delle aree di ricerca e delle traiettorie di sviluppo, va intesa in senso ampio rispetto alla definizione di agglomerato urbano di grande e media dimensione, e si riferisce al concetto di città diffusa e di comunità intelligente (anche attraverso l'aggregazione di piccoli comuni ovvero sistemi metropolitani) nelle quali sono affrontate congiuntamente tematiche riferibili alle sfide sociali emergenti". Nel documento recante *Architettura per le comunità intelligenti: visione concettuale e raccomandazioni alle pubbliche amministrazioni* (vers. 2.0 del 3 ottobre 2012) dell'Agenzia per l'Italia digitale, in <http://www.digitpa.gov.it>, paragrafo 1.1., p. 6, con il termine *Smart City/Community (SC)* si intende quel luogo e/o contesto territoriale ove l'utilizzo pianificato e sapiente delle risorse umane e naturali, opportunamente gestite e integrate mediante le numerose tecnologie ICT già disponibili, consente la creazione di un ecosistema capace di utilizzare al meglio le risorse e di fornire servizi integrati e sempre più intelligenti (cioè il cui valore è maggiore della somma dei valori delle parti che li compongono). Gli assi di sviluppo di una *smart city*, individuati da tale documento, sono molteplici: mobilità, ambiente ed energia, qualità edilizia, economia e capacità di attrazione di talenti e investimenti, sicurezza dei cittadini e delle infrastrutture delle città, partecipazione e coinvolgimento dei cittadini. La connettività diffusa e la digitalizzazione delle comunicazioni e dei servizi sono valutate come condizioni indispensabili per la *smart city*.

⁷⁹ In tal senso il documento dell'Agenzia per l'Italia digitale *Architettura per le comunità intelligenti: visione concettuale e raccomandazioni alle pubbliche amministrazioni*, cit., paragrafo 3, p. 13. Sulle *smart cities* cfr. M. VIANELLO, *Smart cities. Gestire la complessità urbana nell'era di internet*, Rimini, Maggioli, 2013.

apertura⁸⁰. Le comunità intelligenti assumono molteplici significati e si traducono in diverse possibili declinazioni (quali *smart mobility, health, smart economy, social innovation*), sottese e pervase da una necessaria *openness* e da un continuo processo di evoluzione.

Partecipazione e collaborazione devono essere i presupposti delle strategie relative alle *smart cities*. Senza il coinvolgimento dei cittadini la comunità non può essere *smart*, dal momento che gli stessi dati e servizi vivono dell'interazione tra i soggetti che compongono la collettività: cittadini, associazioni e imprese sono i fruitori, che possono monitorare, correggere e migliorare i servizi e possono riutilizzare, condividere e integrare i dati e le informazioni.

La necessità del più ampio coinvolgimento porta la normativa a porre attenzione anche a quella che viene definita "inclusione intelligente", ossia la capacità di rendere fruibili informazioni e servizi senza discriminazioni, garantendo così l'eguaglianza sostanziale dei cittadini⁸¹.

Di recente il d.l. 179/2012 convertito con modificazioni dalla legge 221/2012 ha affidato all'Agenzia per l'Italia digitale il compito di promuovere lo sviluppo e il progresso delle comunità intelligenti, attraverso la definizione di strategie e obiettivi, il coordinamento del processo di attuazione e la predisposizione degli strumenti tecnologici ed economici⁸²; presso l'Agenzia per l'Italia digitale il decreto Crescita 2.0 ha istituito, altresì, il Comitato tecnico delle comunità intelligenti⁸³.

⁸⁰ L'Agenzia per l'Italia digitale nel documento *Architettura per le comunità intelligenti: visione concettuale e raccomandazioni alle pubbliche amministrazioni*, cit., chiarisce che le *smart cities* "devono tener conto della dimensione fondamentale di gestione dell'informazione in un contesto di inclusività e coesione territoriale, di *open government*, di sostenibilità (sotto il profilo IT, energetica e ambientale) e di opportunità di cooperazione e sviluppo tra Pubbliche Amministrazioni, imprese, finanza e cittadini. Gli attori coinvolti infatti sono molteplici come anche gli ambiti organizzativi e tecnologici".

⁸¹ L'art. 20, comma 16, d.l. 179/2012 convertito con modificazioni dalla legge 221/2012 identifica l'"inclusione intelligente" nella capacità, nelle forme e nei limiti consentiti dalle conoscenze tecnologiche, di offrire informazioni nonché progettare ed erogare servizi fruibili senza discriminazioni dai soggetti appartenenti a categorie deboli o svantaggiate e funzionali alla partecipazione alle attività delle comunità intelligenti, definite dal piano nazionale, secondo i criteri stabiliti con decreto del Presidente del Consiglio dei Ministri o del Ministro delegato all'innovazione tecnologica. In merito, l'art. 20, comma 17, d.l. 179/2012 convertito con modificazioni dalla legge 221/2012 precisa che l'accessibilità dei sistemi informatici e l'inclusione intelligente costituiscono principi fondanti del piano nazionale delle comunità intelligenti e dello statuto delle *smart communities*, nonché delle attività di normazione, di pianificazione e di regolamentazione delle comunità intelligenti.

⁸² Art. 20 del d.l. 179/2012 convertito con modificazioni dalla legge 221/2012. A tale scopo l'Agenzia per l'Italia digitale:

- a) predisporre annualmente il piano nazionale delle comunità intelligenti (PNCI) e lo trasmette entro il mese di febbraio al Presidente del Consiglio dei Ministri o al Ministro delegato per l'innovazione tecnologica, che lo approva entro il mese successivo;
- b) predisporre il rapporto annuale sull'attuazione del citato piano nazionale entro il mese di gennaio di ogni anno, avvalendosi del sistema di monitoraggio previsto;
- c) emana le linee guida recanti definizione di standard tecnici, compresa la determinazione delle ontologie dei servizi e dei dati delle comunità intelligenti, e procedurali, nonché di strumenti finanziari innovativi per lo sviluppo delle comunità intelligenti;
- d) istituisce e gestisce la piattaforma nazionale delle comunità intelligenti.

⁸³ L'art. 20 del d.l. 179/2012 convertito con modificazioni dalla legge 221/2012 istituisce presso l'Agenzia per l'Italia digitale il Comitato tecnico delle comunità intelligenti, formato da 11 componenti in possesso di particolari competenze e di comprovata esperienza nel settore delle comunità intelligenti (l'art. 20, comma 2, dettaglia la specifica composizione del Comitato). Le funzioni del Comitato consistono nella proposta all'Agenzia del recepimento di standard tecnici utili allo sviluppo della piattaforma nazionale, nella collaborazione alla supervisione dei documenti che l'Agenzia deve predisporre e nella partecipazione alla definizione dello Statuto. E' prevista infatti l'adozione con d.p.c.m. dello Statuto della cittadinanza intelligente, da redigere sulla base dei criteri previsti all'art. 20, comma 4; la sottoscrizione dello Statuto è condizione necessaria per ottenere la qualifica di comunità intelligente.

La pubblica amministrazione diventa così un'amministrazione digitale aperta, partecipata e collaborativa e si pone come attore protagonista di un nuovo tessuto collettivo e connettivo che diventa quello delle *smart communities*.

6. Gli effetti dell'open government

L'analisi della normativa degli ultimi anni mostra un'apertura crescente ad accogliere nel quadro normativo italiano il concetto di *open government*, attraverso l'incentivazione di strumenti e istituti di trasparenza, partecipazione e collaborazione. Le disposizioni recenti tracciano così l'equipaggiamento necessario affinché l'amministrazione italiana possa assumere il volto di amministrazione digitale aperta, di cui sono chiari i vantaggi.

Sono effetti positivi gli evidenti risparmi di tempo e di risorse economiche e umane dovuti alla logica unitaria e condivisa, che si ritrova nel *cloud computing*, nell'*open source* e nel riuso, ma anche nelle *smart communities*. Far emergere buone pratiche e servirsi dell'apporto collaborativo degli utenti comporta altresì un miglioramento nella qualità dei servizi resi e una maggiore soddisfazione dell'utenza. Si realizzano poi un recupero di efficienza delle amministrazioni pubbliche e un miglioramento della qualità di vita della collettività nel progettare e monitorare servizi adatti a coloro che ne devono fruire. Servizi più veloci e semplici aiutano la competitività e le imprese, che spesso lamentano gli oneri burocratici, la difformità nelle procedure e la lunghezza dei tempi. Trasparenza e *open data* possono contribuire allo sviluppo economico, assicurando inoltre maggiore efficienza ed efficacia all'azione pubblica e permettendo di scongiurare tentativi di corruzione. Tutto questo può favorire nel tempo un recupero di fiducia nelle istituzioni e un guadagno complessivo del sistema Paese. L'apertura, la partecipazione e la collaborazione consentono interazioni inesplorate tra i diversi attori della società, permettendo sinergie fra idee e progetti, assicurando l'emersione dell'intelligenza collettiva e sviluppando soluzioni inedite, possibile fondamento di una nuova crescita economica.

L'analisi condotta mostra che i principi e gli strumenti dell'*open government* sono arrivati a plasmare il recente quadro normativo, caratterizzando l'attuale modello italiano di amministrazione digitale nel senso dell'apertura. Ora è necessario che le norme siano accompagnate da una convinta strategia politica nazionale e da un'attuazione organica e omogenea su tutto il territorio, al fine di far assumere concretamente alle istituzioni italiane il volto di amministrazioni digitali aperte.

Bibliografia

Monografie, collettanee, articoli

- AGNOLONI T., SAGRI M.T., TISCORNIA D., *Open data: nuova frontiera della libertà informatica?*, in "Informatica e diritto", n. 2, 2009, pp. 7-19.
- BELISARIO E., *La nuova Pubblica Amministrazione Digitale*, Rimini, Maggioli, 2009.
- BELISARIO E., COGO G., SCANO R., *I siti web delle pubbliche amministrazioni. Norme tecniche e giuridiche*

-
- dopo le *Linee Guida Brunetta*, Rimini, Maggioli, 2011.
- BUCCOLIERO L., *Il governo elettronico. Modelli, strategie di innovazione ed elementi di valore per una pubblica amministrazione digitale*, Milano, Tecniche Nuove, 2009.
 - COCCAGNA B., ZICCARDI G., *Open data, trasparenza elettronica e codice aperto*, in DURANTE M., PAGALLO U. (a cura di), *Manuale di informatica giuridica e diritto delle nuove tecnologie*, Torino, UTET Giuridica, 2012.
 - CONCAS G., DE PETRA G., GALLUS G.B., GINESU G., MARCHESI M., MARZANO F., *Contenuti aperti beni comuni. La tecnologia per diffondere la cultura*, Milano, McGraw-Hill, 2009.
 - CUNIBERTI M. (a cura di), *Nuove tecnologie e libertà della comunicazione. Profili costituzionali e pubblicistici*, nella collana FRANCESCHELLI V., TOSI E. (a cura di), *Diritto delle nuove tecnologie*, Milano, Giuffrè, 2008.
 - DE PIETRO L. (a cura di), *Dieci lezioni per capire ed attuare l'e-government*, Venezia, Marsilio editori, 2011.
 - DE VIVO M.C., POLZONETTI A., TAPANELLI P., *Open data, Business Intelligence e Governance nella Pubblica Amministrazione*, in D. TISCORNIA (a cura di), *Open data e riuso dei dati pubblici*, in "Informatica e diritto", fasc. 1-2, 2011, pp. 239-262.
 - DI DONATO F., *Lo stato trasparente. Linked open data e cittadinanza attiva*, Pisa, Edizioni ETS, 2011.
 - DOMENICONI P., SCARPIELLO F., *La legge n. 15/2009: fra trasparenza ed eccesso di informazione*, in "Azienditalia – Il Personale", n. 5, 2009, pp. 227- 233.
 - FAINI F., *Dati, siti e servizi in rete delle pubbliche amministrazioni: l'evoluzione nel segno della trasparenza del decreto legislativo n. 235 del 2010*, in TISCORNIA D. (a cura di), *Open data e riuso dei dati pubblici*, in "Informatica e diritto", n.1-2, 2011, pp. 263-286.
 - ID., *La strada maestra dell'open government: presupposti, obiettivi, strumenti*, in "Cyberspazio e diritto", n. 2, 2013, pp. 213-240.
 - FLICK C., CIGNONI G.A., AMBRIOLA V., *Il riuso del software nella pubblica amministrazione*, in "Diritto dell'internet", n. 1, 2008, p. 85 e seguenti.
 - GIANFELICI C., *Le indagini di customer satisfaction nelle amministrazioni pubbliche: finalità, metodologia e strumenti*, in "Azienditalia", n. 1, 2009, pp. 1-29.
 - LÉVY P., *L'intelligenza collettiva. Per un'antropologia del cyberspazio*, trad.it, Milano, Feltrinelli, 1996, p. 36 e seguenti.
 - LIMONE D. A., *Elementi di diritto dell'informatica*, Lecce, Editrice Salentina, 1999.
 - ID., *Politica e Normativa Comunitaria per la Società dell'Informazione (1990-2010)*, in "Rivista elettronica di Diritto, Economia, Management", n. 1, 2010, rivista telematica in http://www.giuritecne.it/wp-content/uploads/2011/01/rivista-elettronica_1_2010.pdf.
 - MAGGIPINTO A., *Internet e Pubbliche amministrazioni: quale democrazia elettronica?*, in "Il Diritto dell'Informazione e dell'Informatica", n. 1, 2008, pp. 45-58.
 - MANCARELLA M., *Profili negoziali e organizzativi dell'amministrazione digitale*, Trento, Tangram Edizioni Scientifiche, collana Isegoria, 2008.
 - ID., *La Società dell'Informazione tra eGovernment e principio di sussidiarietà*, in "Rivista elettronica di Diritto, Economia, Management", n. 1, 2010, rivista telematica in http://www.giuritecne.it/wp-content/uploads/2011/01/rivista-elettronica_1_2010.pdf.

content/uploads/2011/01/rivista-elettronica_1_2010.pdf.

- MARZANO F. *La trasparenza nella Pubblica Amministrazione passa dall'Open Data o l'Open Data passa dalla trasparenza?*, in D. TISCORNIA (a cura di), *Open data e riuso dei dati pubblici*, in “Informatica e diritto”, fasc. 1-2, 2011, pp. 287-303.
- PIRAS P., *Servizi pubblici e nuove tecnologie*, in “Il diritto dell’informazione e dell’informatica”, n. 2, 2006, pp. 93-99.
- PREITE G., *Habeas data tra sicurezza e privacy: quale politica per i nuovi diritti?*, in SIRIMARCO M. (a cura di) “*Info-ius. Problemi e prospettive dell’informatica giuridica*”, Roma, Nuova Cultura, 2010, pp. 279-304.
- PROSPERETTI E., *Gli obblighi di assicurare la custodia e la sicurezza dei dati in un sistema cloud*, in CASSANO G., SCORZA G., VACIAGO G., *Diritto dell’internet. Manuale operativo. Casi, legislazione, giurisprudenza*, Padova, Cedam, 2013, pp. 675-690.
- RAZZANTE R., *Manuale di diritto dell’informazione e della comunicazione. Privacy, diffamazione e tutela della persona. Libertà e regole nella Rete*, 5° ed., Padova, Cedam, 2011, p. 419 e seguenti.
- SARTOR G., *L’informatica giuridica e le tecnologie dell’informazione – Corso d’informatica giuridica*, 2° edizione, Torino, Giappichelli, 2010.
- SITZIA S., *Informazione, nuove tecnologie e cambiamenti relazionali fra PA e cittadini*, in “Diritto dell’Internet”, n. 6, 2006, pp. 615-618.
- TARALLO P. (a cura di), BUONGIOVANNI A., MARZANO F., TESI E., ZECCHI P., *Digital divide. La nuova frontiera dello sviluppo globale*, Milano, Franco Angeli, 2003.
- TEDESCHI M., *E-Democracy*, in DE PIETRO L. (a cura di), *Dieci lezioni per capire ed attuare l’e-government*, Venezia, Marsilio editori, 2011, p. 155 e seguenti.
- TISCORNIA D. (a cura di), *Open data e riuso dei dati pubblici*, in “Informatica e diritto”, fasc. 1-2, 2011.
- VIANELLO M., *Smart cities. Gestire la complessità urbana nell’era di internet*, Rimini, Maggioli, 2013.

Documenti

- AGENZIA PER L’ITALIA DIGITALE, *Architettura per le comunità intelligenti: visione concettuale e raccomandazioni alle pubbliche amministrazioni*, versione 2.0, 3 ottobre 2012, in <http://www.digitpa.gov.it>.
- ID., circolare n. 61 del 29 marzo 2013, *Disposizioni del decreto legge 18 ottobre 2012, n. 179, convertito con modificazioni dalla L. 17 dicembre 2012, n. 221 in tema di accessibilità dei siti web e servizi informatici. Obblighi delle pubbliche Amministrazioni*, in <http://www.digitpa.gov.it>.
- ID., *Linee guida nazionali per la valorizzazione del patrimonio informativo pubblico (secondo semestre 2013)*, 31 luglio 2013, in <http://www.digitpa.gov.it>.
- CIVIT (COMMISSIONE INDIPENDENTE PER LA VALUTAZIONE, LA TRASPARENZA E L’INTEGRITÀ DELLE AMMINISTRAZIONI PUBBLICHE), delibera n. 105 del 14 ottobre 2010, *Linee guida per la predisposizione del Programma triennale per la trasparenza e l’integrità*, in <http://www.civit.it>.
- ID., delibera n. 2 del 5 gennaio 2012, *Linee guida per il miglioramento della predisposizione e l’aggiornamento del Programma triennale per la Trasparenza e Integrità*, in <http://www.civit.it>.
- ID., delibera n. 50 del 4 luglio 2013, *Linee guida per l’aggiornamento del Programma triennale per la*

-
- trasparenza e l'integrità 2014-2016*, in <http://www.civit.it>.
- COMMISSIONE EUROPEA, comunicazione del 12 dicembre 2011, *Dati aperti. Un motore per l'innovazione, la crescita e una governance trasparente*, in <http://eur-lex.europa.eu>.
 - DIGITPA, PRESIDENZA DEL CONSIGLIO DEI MINISTRI – DIPARTIMENTO DELLA FUNZIONE PUBBLICA, DIPARTIMENTO PER LA DIGITALIZZAZIONE E L'INNOVAZIONE TECNOLOGICA, FORMEZPA, *Linee guida per i siti web della PA (art. 4 della Direttiva n. 8/2009 del Ministro per la pubblica amministrazione e l'innovazione)*, 26 luglio 2010, aggiornate il 29 luglio 2011, in <http://www.funzionepubblica.gov.it>.
 - DIGITPA, *Raccomandazioni e proposte sull'utilizzo del cloud computing nella pubblica amministrazione*, versione 2.0, 28 giugno 2012, in <http://www.digitpa.gov.it>.
 - MINISTERO DELL'ISTRUZIONE, DELL'UNIVERSITÀ E DELLA RICERCA – MIUR, decreto direttoriale n. 391/Ric. del 5 luglio 2012, *Avviso per la presentazione di idee progettuali per Smart Cities and Communities and Social Innovation*, in <http://www.istruzione.it>.
 - PRESIDENZA DEL CONSIGLIO DEI MINISTRI – DIPARTIMENTO DELLA FUNZIONE PUBBLICA, direttiva n. 8 del 26 novembre 2009, *Direttiva del Ministro per la pubblica amministrazione e l'innovazione per la riduzione dei siti web delle pubbliche amministrazioni e per il miglioramento della qualità dei servizi e delle informazioni online al cittadino*, in <http://www.funzionepubblica.gov.it>.
 - ID., circolare n. 2 del 19 luglio 2013, recante *D.lgs. n. 33/2013 – Attuazione della trasparenza*, in <http://www.funzionepubblica.gov.it>.

I NUOVI SCENARI DELLA SOCIETÀ DELL'INFORMAZIONE: ASPETTI POLITICI, GIURIDICI, AMMINISTRATIVI E TECNICI DIBATTITO E CHIUSURA DEL CONVEGNO

Donato A. Limone

 *Multimedia*



Clicca sull'immagine o fotografa il QrCode
per accedere al MediaBook CLIOedu

