Rivista elettronica di Diritto, Economia, Management

Numero 3 - 2015 • Edizione multimediale

Parte Prima - a cura di Giuseppe Vaciago
Atti del Convegno: "Informatica giuridica e Diritto dell'informatica. Esperienze nazionali ed europee"
Como, 3 ottobre 2014 - Università degli Studi dell'Insubria

Parte Seconda - a cura di Giovanni Grea
Contributi in materia di protezione dei dati personali

Parte Terza
Contributi sul Risk management

FONDATA E DIRETTA DA
DONATO A. LIMONE

CLIOEDU®

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

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

Anno V, n. 3/2015
ISSN 2039-4926
Autorizzazione del Tribunale civile di Roma N. 329/2010 del 5 agosto 2010
Editor ClioEdu
Roma - Lecce

Indice

Parte Terza
Contributi sul Risk Management

Editoriale

Il numero 3/2015 è strutturato in 3 parti: la prima, riporta gli atti (in modalità multimediale) della giornata di studio "Informatica giuridica e Diritto dell'informatica: esperienze nazionali ed europee" (venerdì 3 ottobre 2014, Università degli Studi dell'Insubria, Como, in collaborazione con ANDIG), organizzato dal prof. Giuseppe Vaciago; la seconda, dedicata alla tematica della protezione dei dati personali, curata da Giovanni Crea; la terza, comprende due contributi in materia di *risk management.*

Il Direttore della Rivista
Donato A. Limone

Istruzioni per la lettura

Gli interventi dei relatori del Convegno ANDIG "Informatica giuridica e Diritto dell'informatica: esperienze nazionali ed europee" tenutosi a Como il 3 ottobre 2014 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

Virginia Alongi

Abilitata all'esercizio della professione forense presso la Corte d'Appello di Roma, collabora con lo Studio Prosperetti & Associati dove si occupa di privacy, TMT e IP. Ha collaborato con studi internazionali occupandosi di diritto amministrativo. Attualmente è consulente giuridico presso l'AGENAS ("Agenzia Nazionale per i Servizi Sanitari Regionali"). È autrice di pubblicazioni su argomenti di diritto amministrativo e diritto dell'energia.

E-mail: v.alongi@studioprosperetti.it

Fabrizio Corona

Dottore in giurisprudenza, docente a contratto di Informatica Giuridica presso l'Università LUISS Guido Carli e collaboratore Universitario nella cattedra di Logica ed Informatica Giuridica presso l'Università degli studi di Napoli Federico II.

E-mail: fabrizio.corona@inwind.it

Antonio Coviello

Ricercatore presso l'IRISS. È laureato in Economia e Commercio presso la Facoltà di Economia "Federico II" di Napoli. Nell'ambito dell'area di ricerca "Innovazione e management dei servizi", è responsabile del progetto di ricerca denominato "L›innovazione per la crescita dei servizi assicurativi e del risk management". Dal giugno 2007 (anno di ingresso nel CNR) svolge attività di ricerca nel campo delle Economia e Gestione delle Imprese Assicurative. L'attività di studio si concretizza lungo due assi di ricerca principali: un primo asse con obiettivi specifici riferiti all'innovazione per lo sviluppo dei servizi assicurativi ed un secondo ascrivibile all'identificazione degli approcci gestionali derivanti dai rischi originati da eventi naturali. In riferimento al sempre e più attuale argomento dei danni derivanti da eventi naturali, ha analizzato in particolare il ruolo e il comportamento del Risk Management in relazione alla assunzione di adeguate coperture assicurative per rischi c.d. catastrofali. Per il secondo asse di ricerca, ha svolto e svolge studi relativi all'individuazione di soluzioni concernenti l'Evoluzione dei canali distributivi (ICT) delle Imprese assicurative e il lancio di nuovi servizi market-driven e/o technology-driven. È stato responsabile del progetto di ricerca denominato "L'innovazione per la crescita dei servizi assicurativi e del risk management", e coordina un gruppo di lavoro multisciplinare composto da qualificati esperti in materia (Enea, Ania ed altri enti assicurativi e riassicurativi). È professore universitario a contratto, attualmente insegna Marketing assicurativo" presso l"Università Suor Orsola Benincasa. Ha pubblicato numerosi scritti in materia

assicurativa, tra cui monografie adottate in diverse Università italiane.

E-mail: a.coviello@iriss.cnr.it

Giovanni Crea

Economista, è professore a contratto di "Psicologia economica e Information and communication technologies" presso l'Università Europea di Roma. È direttore della Collana "Quaderni di Diritto ed economia delle comunicazioni e dei *media*" (Aracne editrice). È autore di numerose pubblicazioni scientifiche su argomenti riguardanti il settore delle *Information and communication technologies*.

E-mail: gio2010.crea@gmail.com

Giovanni Di Trapani

Ricercatore universitario. Ha conseguito il Dottorato - PhD. in "Economia e gestione delle Aziende Pubbliche" presso la Facoltà di Economia dell'Università di Salerno ed è laureato in Economia e Commercio conseguita presso la Facoltà di Economia "Federico II" di Napoli. Svolge nell'ambito dell'area di ricerca "Innovazione e management dei servizi" attività di studio lungo due assi di ricerca principali: un primo asse con obiettivi specifici riferiti all'innovazione per lo sviluppo dei servizi assicurativi ed un secondo ascrivibile all'identificazione degli approcci gestionali derivanti dai rischi originati da eventi naturali. Svolge attività di ricerca nel campo delle Economia e Gestione delle Imprese Assicurative a partire dal giugno 2010, ed a tal proposito, in riferimento al sempre e più attuale argomento dei danni derivanti da eventi naturali, ha portato avanti studi ed analisi con l'obiettivo di analizzare il ruolo e il comportamento del Risk Management in relazione alla assunzione di adeguate coperture assicurative per rischi c.d. catastrofali. Nel recente passato ha svolto studi relativi all'individuazione di soluzioni concernenti l'Evoluzione dei canali distributivi (ICT) delle Imprese assicurative e il lancio di nuovi servizi market-driven e/o technology-driven. In precedenza, fino al maggio del 2010, il sottoscritto ha affrontato gli argomenti connessi con il Management del Turismo e dei Beni Culturali, con particolare riferimento alla gestione, fruizione e valorizzazione economica del Patrimonio Culturale. È componente del Comitato Editoriale della Rivista Paradox. È, da dieci anni, Professore a Contratto di Statistica Economica e Statistica del Turismo presso l'Università Telematica PEGASO. Ha pubblicato numerosi scritti in materia assicurativa e mirati allo studio quantitativo e qualitativo di fenomenologie turistiche innovative.

E-mail: ditrap@gmail.com

Anna Esposito

Laureata in Scienze della Politica conseguita presso la Seconda Università degli Studi di Napoli; è, altresì, laureata con qualifica di Consulente del Lavoro presso l'Università degli Studi di Siena.

Ha svolto attività di ricerca, per lo più lungo due assi principali: un primo asse che con

obiettivi specifici riferiti all'innovazione per lo sviluppo dei servizi ed un secondo ascrivibile all'identificazione degli approcci statistici e gestionali derivanti dai rischi stessi. A partire da giugno 2012, ha svolto, tra l'altro, attività di ricerca finalizzata al supporto statistico quantitativo per l'elaborazione di un piano di valorizzazione di importanti siti archeologici. Infine, ha condotto, nell'ambito del progetto ADAPT II Fase, presso l'EFSA - Campania un analisi della letteratura ed un supporto alle indagini empiriche, fondate su case study, focalizzando la propria attenzione sull'overview dello stato di internazionalizzazione delle imprese italiane. Svolge attività di ricerca, per conto di clienti pubblici e privati, inerente la costruzione di database di marketing mediante l'aggregazione di dati qualitativi, raccolti tramite attività di sondaggi, ed attività di customer care. È Professore a Contratto di Statistica Economica presso l'Università Telematica PEGASO.

E-mail: annaesposito38@virgilio.it

Francesca Ferrari

Nell'anno accademico 1992-1993 ha conseguito la laurea in Giurisprudenza presso l"Universita degli Studi di Pavia discutendo una tesi dal titolo «Fatti bruti e fatti istituzionali» e riportando la votazione di 110/110 e lode. Nel 1996 ha conseguito una borsa di studio che le ha permesso di frequentare per otto mesi la Harvard University (Cambridge-Massachussets, USA), quale visiting researcher e di approfondire gli studi in materia di evidence, in particolare con il prof. John Mansfield, ai fini della redazione della tesi di dottorato. Nel 1997 ha conseguito il titolo di dottore in ricerca in diritto processuale civile. Nel 1998 ha vinto una borsa di studio post dottorato e da allora collabora attivamente con la cattedra di Diritto Processuale Civile dell"Universitàˋ degli Studi di Milano Nell»ottobre del 2003 Francesca Ferrari, a seguito di procedura di valutazione comparativa ha vinto un posto di ricercatore presso l»Universitàˋ degli Studi dell»Insubria ed è entrata in servizio, a seguito del blocco delle assunzioni, il 1Â° marzo 2005.

E-mail: francesca.ferrari@uninsubria.it

Michele Iaselli

Avvocato, è vicedirigente del Ministero della Difesa, docente a contratto di informatica giuridica presso l'Università LUISS e collaboratore Universitario nella cattedra di Logica ed Informatica Giuridica presso l'Università degli studi di Napoli Federico II. È Presidente dell'Associazione Nazionale per la Difesa della Privacy (ANDIP).

E-mail: info@micheleiaselli.it

Daniela M. Intravaia

Dirigente dell'Area Progettazione e Programmazione Europea e Internazionale di AgID, Agenzia per l'Italia Digitale, dal gennaio 2016. Ha lavorato nel Ministero della

giustizia dal 1981 al 2015, ricoprendo diversi ruoli professionali. Dal 2000 in area informatica giudiziaria, è stata dirigente territoriale e dal 2012 al 2014 direttore generale per i sistemi informativi, dove ha realizzato il dispiegamento nazionale di Processo Civile Telematico, l'aggiornamento dei registri penali (dal 1989), il parziale consolidamento delle sale server da circa 200 a 27, gestendo bilanci inferiori a quelli degli anni precedenti.

E-mail: intravaia@agid.gov.it

Alesssandro Mantelero

Professore aggregato di Diritto Privato e di Innovation & International Transactions Law presso il the Politecnico di Torino. È inoltre Director of Privacy presso il NEXA-Center for Internet & Society, part-time expert presso la Nanjing University of Information Science & Technology e coordinatore del Double Degree program in Management and IP Law (Politecnico di Torino – Tongji University of Shanghai). Nel 2016, è stato nominato Expert Consultant dal Consiglio d'Europa per redigere le line guida sulla protezione dei dati personali nel contesto dei Big Data. Ha svolto attività di ricerca presso le seguenti università: Harvard (Berkman Center for Internet & Society, visiting researcher), Oxford (OxfordInternet Institute, visiting fellow), Nanjing University of Information Science & Technology (School of Public Administration, visiting professor), Universitat Oberta de Catalunya (Internet Interdisciplinary Institute, visiting professor).

E-mail: alessandro.mantelero@polito.it

Andrea Orlandoni

Iscritto all'Ordine degli Avvocati di Como ed è specializzato nella risoluzione di contenziosi in materia di diritto commerciale, societario, infortunistica e risarcimento danni, responsabilità civile. Si occupa di tutte quelle problematiche che riguardano la responsabilità professionale e la responsabilità civile in genere.

E-mail: info@avvorlandoni.it

Filippo Pappalardo

Èstato per diversi anni cultore della materia di informatica giuridica presso l'Università degli Studi di Milano, Milano-Bicocca e Uninsubria Como. Dal 2007 si occupa di Processo Telematico come consulente esterno per il Ministero della Giustizia (e dal 2008 per l'Unione Lombarda degli Ordini Forensi nel settore civile (estensione territoriale PCT in Lombardia). È Coordinatore dell'Ufficio Innovazione dell'Ordine degli Avvocati Milano e responsabile della formazione avvocati in ambito PCT per l'Ordine degli Avvocati di Milano, partecipa inoltre al gruppo di lavoro operativo per l'estensione ad altre procedure del progetto PCT a Milano e in Lombardia. Fa parte del comitato ideatore di Agenda Digitale Giustizia: www.agendadigitalegiustizia.it

E-mail: fil.pappalardo@gmail.com

Giulio Pascali

Avvocato in Roma, collabora con lo Studio Prosperetti & Associati quale componente delle aree TMT/MEDIA. Ha conseguito nel 2010 la specializzazione in "diritto e gestione della proprietà intellettuale, della concorrenza e delle comunicazioni" presso l'Università "LUISS Guido Carli" di Roma. Ha collaborato alla ricerca ISBUL (Infrastrutture a Banda Larga e Ultra Larga) dell'AGCOM, all'Osservatorio Agenda Digitale dell'ISIMM Ricerche ed è autore di pubblicazioni scientifiche nei settori delle ICT, della privacy e dei nuovi *media*.

E-mail: g.pascali@studioprosperetti.it

Gianni Penzo Doria

Direttore Generale dell'Università degli Studi dell'Insubria. Di formazione classica, si è occupato dei problemi connessi all'introduzione del protocollo informatico (ancora nel 1995), della firma digitale, della classificazione e fascicolatura, dei sistemi informativi sia nel settore pubblico che nel settore privato, trattando prevalentemente le tematiche inerenti alla trasparenza amministrativa, all'informatica giuridica, alla diplomatica dei documenti pubblici e delle collegialità amministrative. Ha riservato una cospicua mole di attività alla reingegnerizzazione dei procedimenti amministrativi e dei sistemi di workflow management e ha scritto una quarantina di saggi sui temi dell'amministrazione digitale, dell'organizzazione degli archivi, dell'albo on-line, della PEC e dei rapporti tra trasparenza e sistema documentale. È componente del Comitato tecnico-scientifico degli archivi in seno al Ministero dei beni e della attività culturali e del turismo, Coordinatore nazionale di Titulus Scuola (http://scuola.titulus.it), il progetto del MiBACT per la digitalizzazione degli archivi scolastici italiani e Responsabile scientifico del progetto Procedamus (www.procedamus.it), in tema di procedimenti amministrativi per le università e per gli enti di ricerca. Collabora con AgID sui temi della pubblicità legale.

E-mail: gianni.penzodoria@gmail.com

Andrea Rossetti

Professore associato confermato di Filosofia del diritto all'Università di Milano-Bicocca, dove insegna anche Informatica giuridica (insegnamento che dal 2007 al 2012 ha ricoperto anche alla Statale di Milano). I suoi lavori principali riguardano lo studio della possibilità dell'uso di sistemi formali per l'espressione del diritto e l'ontologia degli oggetti sociali e immateriali (Deontica in Jean Louis Gardies. Logica e ontologia degli atti sociali, 1999; Modi deontici nell'ordinamento giuridico, 2004). Attualmente, in questo ambito, i suoi studi sono concentrati sul concetto di "documento giuridico telematico". Dal 1999, si occupa di Informatica giuridica; in particolare ha dedicato alcuni saggi di carattere divulgativo all'idea di "openness" nell'ambito dell'ICT; ha curato ed introdotto il manuale: Legal Informatics. Dirige ReF-Recensioni Filosofiche, la rivista italiana dedicata alla recensione di libri di filosofia.

E-mail: andrea.rossetti@unimib.it

Giovanni Sartor

Professore di informatica giuridica e teoria del diritto presso l'Istituto Universitario Europeo di Firenze e professore ordinario di informatica giuridica presso l'Università di Bologna. Dopo aver ottenuto il dottorato in Scienze giuridiche presso l'Istituto universitario europeo di Firenze, è stato funzionario della Corte di giustizia dell'Unione europea, ricercatore al CNR (ITTIG, Firenze), e titolare della cattedra in Jurisprudence presso la Queen's University di Belfast. È stato presidente della International Association for Artificial Intelligence and Law. È coeditor delle riviste Artificial Intelligence and Law e Ratio Juris. I suoi interessi scientifici comprendono la teoria del diritto, la logica, la teoria dell'argomentazione, la logica deontica e modale, la programmazione logica, i sistemi multiagente, il diritto dell'informatica, la protezione dei dati, il commercio elettronico, diritto e tecnologia, diritto dell'aviazione, diritti umani.

E-mail: giovanni.sartor@unibo.it

Giuseppe Vaciago

Avvocato esperto in diritto penale societario e delle nuove tecnologie. ha maturato una considerevole esperienza nella consulenza finalizzata alla redazione dei compliance program ai sensi del D.lgs. 231/01. Ha prestato la sua attività professionale per alcune importanti società nazionali e internazionali nel settore IT.Ha conseguito un PHD in Digital Forensics all'Università degli Studi di Milano Bicocca ed è docente di informatica giuridica presso l'Università degli Studi dell'Insubria. Ha frequentato in qualità di Visiting Scholar la Stanford Law School e la Fordham Law School di New York. Ha partecipato a numerosi convegni a livello nazionale e internazionale. È fellow del Nexa Center di Torino, del Cybercrime Institute di Colonia ed è socio fondatore del Tech and Law Center di Milano. È autore di numerose pubblicazioni di carattere universitario tra cui "Computer Crimes", "Digital Evidence" e "Modelli di organizzazione gestione e controllo ai sensi del D.lgs. 231/01".

E-mail: giuseppe.vaciago@uninsubria.it

Giorgio Maria Zamperetti

Professore ordinario nel Dipartimento di Diritto, Economia e Culture (già Facoltà di Giurisprudenza) dell'Università degli Studi dell'Insubria, sede di Como (S.S.D. IUS/04). All'Insubria è titolare dei corsi di Diritto commerciale progredito nel corso di laurea in giurisprudenza e di Law and Humanities nel corso di laurea in Scienze della mediazione linguistica; è stato docente nel Master in etica e responsabilità sociale negli affari e nelle professioni e ha insegnato diritto dell'informatica; ha inoltre insegnato nel Master in contrattualistica pubblica presso il Politecnico di Milano e tenuto docenze presso numerose istituzioni. Nel campo del diritto dell'informatica ha fondato, insieme a docenti di altri atenei,ADINT - Associazione per il diritto delle nuove tecnologie, di cui è attualmente presidente.

Email: giorgio.zamperetti@uninsubria.it

PARTE PRIMA

Atti della Giornata di Studi
“Informatica giuridica e Diritto dell’informatica: esperienze nazionali ed europee”
Università degli Studi dell’Insubria
in collaborazione con ANDIG
3 ottobre 2014, Como.
Coordinamento scientifico del prof. Giuseppe Vaciago

Introduzione

La crescita esponenziale dell'utilizzo delle nuove tecnologie nel settore pubblico e privato impone una riflessione sull'adeguatezza dell'attuale framework legislativo a livello nazionale ed europeo in tema di diritto dell'informatica.
Se a livello Europeo, in attesa che le proposte di direttive e di regolamenti trovino la luce, alcune significative pronunce della Corte di Giustizia hanno fornito un indirizzo interpretativo su alcuni settori come l'e-commerce, la privacy e il copyright, a livello nazionale, l'avvio ufficiale del processo civile telematico e il regolamento AGCOM a tutela del diritto d'autore sono stati i due più rilevanti interventi in materia.
La Giornata di Studi ha preso in esame i due differenti approcci con l'obiettivo di fornire un'analisi comparatistica della materia, ma anche di dare soluzioni pratiche su temi sicuramente rilevanti come il processo civile telematico, la fatturazione elettronica e il diritto all'oblio.
Durante la sessione mattutina, sono state presentate le principali novità in tema di digitalizzazione della Pubblica Amministrazione, moderando alcuni tra i relatori più esperti in materia.
Nel pomeriggio, invece, sono stati analizzati i più rilevanti casi della Corte di Giustizia dell'Unione Europea in materia.

Giuseppe Vaciago

Ontologia sociale del documento digitale

Andrea Rossetti

Multimedia

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

La responsabilità dell'internet service provider e la disciplina del commercio elettronico

Alessandro Mantelero

Multimedia

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

Il dirttto all'oblio e i motori di ricerca

Giovanni Sartor

Multimedia

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

L'invalidità della Direttiva sulla Data Retention

Giuseppe Vaciago

Multimedia

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

Il bilanciamento di interessi tra copyright e diritti fondamentali dell'individuo

Chiara Alvisi

Multimedia

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

Introduzione alla giornata di studi

Giorgio Maria Zamperetti

Multimedia

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

Il Processo civile telematico. L'interpretazione delle norme processuali e tecniche

Andrea Orlandoni

Multimedia

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

Apertura della giornata di studi

Daniela Intravaia

Multimedia

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

Conclusioni sessione mattutina

Daniela Intravaia, Francesca Ferrari, Andrea Orlandoni

Multimedia

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

PCT Obbligatorietà

Filippo Pappalardo

Multimedia

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

Il processo telematico alla luce delle più recenti modifiche legislative

Francesca Ferrari

Multimedia

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

Le professioni del digitale per una coalescenza interprofessionale: giuristi, informatici, archivisti e diplomatisti

Gianni Penzo Doria

Multimedia

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

PARTE SECONDA

Contributi in materia di protezione dei dati personali.

A cura di Giovanni Crea

N. 3 - 2015 · pp. 26-36

Identificazione elettronica e servizi fiduciari: verso un'identita digitale europea

Virginia Alongi

Abstract: Oggi più che mai lo sviluppo economico e sociale di un Paese passa inevitabilmente dalla rete internet. Le interazioni e le transazioni elettroniche costituiscono il principale – destinato a divenire l'esclusivo – canale di interconnessione tra cittadini, imprese e autorità pubbliche. Tuttavia, le regole giuridiche che presidiano ed informano gli ambienti *on-line* non riescono a tenere il passo delle regole del mercato – sia interno che globale – che mutano velocemente e rendono incerto il *playground* dei servizi elettronici pubblici e privati, dell' *E-business* e del commercio elettronico nell'Unione Europea.

La carenza del canone di certezza giuridica dell'attuale regime di identificazione elettronica nell'ambito dei servizi fiduciari, alimenta la diffidenza sia degli operatori commerciali sia dei soggetti istituzionali che pertanto sono restii ad effettuare transazioni elettroniche e ad adottare e promuovere servizi innovativi.

Scopo del presente contributo sarà pertanto quello di illustrare le novità introdotte dal legislatore europeo con il c.d. Regolamento e-IDAS relativamente all'identificazione elettronica delle persone fisiche e giuridiche che interagiscono nel mercato interno attraverso transazioni elettroniche.

Abstract: Nowadays the economic and social development of a Country inevitably comes from the Internet. Interactions and electronic transactions are supposed to become in a near future the exclusive interconnection channel between citizens, businesses and public authorities. However, the legal rules that govern and inform the on-line environments fail to keep up with domestic and global market rules which are change quickly defining an uncertain playground of electronic public and private services related to the E-business and e-commerce in the European Union. The lack of legal certainty of the current electronic identification system in the context of trust services, generate the dis-trust of both the traders and the institutional actors who are therefore reluctant to make electronic transactions, adopt and promote innovative services. Therefore the purpose of this contribution will be to illustrate the changes introduced by the European legislator with the e-IDAS Regulation relatively electronic identification of individuals and legal entities that interact in the market through electronic transactions.

Parole chiave: identità digitale, firma elettronica, servizi fiduciari, transazioni elettroniche, Agenda digitale Europea.

Articolo pervenuto il 10 febbraio 2015, approvato il 20 febbraio 2015

Sommario: 1. Introduzione - 2. L'identità digitale e l'identificazione elettronica – 3. I livelli di garanzia – 4. Gli *e-Trust services* – 5. Il Regolamento e-IDAS e il sistema italiano SPID: un confronto. – 6. Conclusioni

1. Introduzione

Il 28 agosto 2014 è stato pubblicato nella Gazzetta ufficiale dell'Unione europea il Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio del 23 luglio (di seguito,"Regolamento") in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno.

Il Regolamento, entrato parzialmente in vigore il 17 settembre di quest'anno, - a mente dell'art. 52 infatti si applicherà integralmente a partire dal 1° luglio 2016 per consentire agli Stati membri di adeguare le rispettive legislazioni nazionali - abroga la direttiva 1999/93/CE concernente le firme elettroniche ed al relativo impiego e riconoscimento giuridico nell'ambito degli Stati membri. Non è di poca rilevanza la scelta del legislatore europeo, il quale optando per strumento legislativo regolamentare in luogo della direttiva, ha voluto dare un forte segnale: il Regolamento infatti, obbligatorio in tutti i suoi elementi, sarà direttamente applicabile in ciascuno degli Stati membri.

Strutturato in 6 Capi, il Regolamento si compone di 52 articoli e 4 Allegati (Allegato I "*Requisiti per i certificati qualificati di firma elettronica*"; Allegato II "*Requisiti per i dispositivi per la creazione di una firma elettronica qualificata*"; Allegato III "*Requisiti per i certificati qualificati dei sigilli elettronici*"; Allegato IV "*Requisiti per i certificati qualificati di autenticazione di siti web*".

Il Regolamento e-IDAS *(electronic Identification Authentication and Signature*), è costruito su due principi fondanti e generali: il principio di reciprocità ed il principio del mercato interno[1].

Per quanto concerne il principio di reciprocità, il Regolamento individua e definisce le regole che consentono e favoriscono il reciproco riconoscimento degli strumenti di identificazione elettronica (firme elettroniche, sigilli elettronici, validazioni temporali elettroniche, documenti elettronici, servizi elettronici di recapito certificato e servizi relativi ai certificati di autenticazione di siti web) delle persone fisiche e giuridiche.

Allo stesso tempo, in virtù dell'altrettanto generale principio del mercato interno, il Regolamento non impone restrizioni in relazione alla prestazione di servizi fiduciari che, al contrario, se conformi alle relative prescrizioni, godono della libera circolazione nel mercato interno in pieno spirito europeista.

---

[1] Con l'Atto per il Mercato Unico II, approvato il 3 ottobre 2012 e che prosegue nella direzione indicata stabilita dall'Atto per il Mercato Unico I dell'1 Aprile 2011, la Commissione ha proposto 12 azioni prioritarie per sviluppare ulteriormente il mercato unico e valorizzarne le potenzialità. Le azioni si concentrano su quattro fattori principali di crescita, occupazione e fiducia: reti integrate, mobilità transfrontaliera di cittadini e imprese, economia digitale e azioni atte a rafforzare la coesione e i vantaggi per i consumatori e ciò al fine di creare un mercato unico più completo e maggiormente integrato.

Ai sensi dell'art. 6, infatti, purché siano rispettate le condizioni ivi fissate, i mezzi di identificazione ed autenticazione elettronica per mezzo dei quali è possibile accedere ad un servizio prestato da un organismo del settore pubblico *on-line* in uno Stato Membro, sono riconosciuti in un altro Stato membro ai fini dell'autenticazione transfrontaliera.
La frammentazione del mercato digitale, la mancanza di inter-operatività e l'aumento dei c.d. *computer crimes* [2] costituiscono, di fatto, i principali e maggiori ostacoli che impediscono ai cittadini dell'Unione di godere dei vantaggi di un mercato unico digitale e dei relativi servizi di natura transfrontaliera.
In molti casi, infatti, i cittadini non sono in grado di avvalersi dello strumento dell'identificazione elettronica proprio perché i regimi nazionali di identificazione elettronica dello Stato membro di appartenenza non sono riconosciuti in altri Stati membri.
Il Regolamento sull'identità digitale e servizi fiduciari (e-TS – *Electronic Trust Services*) pertanto predispone un sistema di regole comuni per tutti gli Stati membri al fine di abbattere barriere ed ostacoli che si frappongono nei settori essenziali dell'economia, giorno dopo giorno sempre più digitale.
L'ambito d'applicazione del Regolamento interessa i regimi di identificazione elettronica che siano stati notificati[3], a norma dell'art. 9 del Regolamento, da uno Stato membro nonché ai prestatoti di servizi fiduciari stabiliti nel territorio dell'Unione; al contrario, il Regolamento non trova applicazione in relazione a sistemi chiusi a rilevanza meramente nazionale.
Altri due principi cardine sui quali è costruito il Regolamento sono quelli di interoperabilità e di cooperazione che, in forza dell'art. 12, risultano essere concepiti funzionalmente alla promozione ed al raggiungimento di un elevato livello di fiducia e di sicurezza nelle reti. Scopo del Regolamento infatti è anche quello di conseguire un sistema univoco e comune di neutralità tecnologica, di tutela protezione dei dati personali, di livelli di garanzia, di disposizioni per la risoluzione di eventuali controversie. Interoperabilità e cooperazione sono i meccanismi che troveranno piena attuazione entro la fine del 2015.
Il Regolamento, che si pone in perfetta armonia con gli obiettivi dell'Agenda Digitale

---

[2] Sulla criminalità informatica, la Convenzione di Budapest del 23 novembre 2011, ratificata dall'Italia con la legge n. 48 del 4 aprile 2008 stabilisce a livello internazionale norme e linee guida da seguire al fine di prevenire e combattere la criminalità informatica. Per una panoramica generale sui *computers crimes* si veda, G. Sisto e A. Casillo "*Il fenomeno dei computer crimes – i crimini informatici nella legislazione italiana, in Diritto delle nuove tecnologie informatiche e dell'internet*, a cura di G. Cassano, 2002, Milano, 1375. Una certa dottrina specializzata del settore ha definito i *computers crimes* come "*ipotesi delittuose commesse mediante l'impiego di strumenti informatici e telematici, nonché di ipotesi delittuose nelle quali il mezzo informatico e telematico rappresenta il bene leso o messo in pericolo",* Bravo, "*Crimini informatici e utilizzo dei mezzi di ricerca della prova nella conduzione delle indagini*", in Riv. Giur. Polizia, 1998, 711.

[3] Il Regolamento stabilisce che i regimi di identificazione elettronica devono essere *notificati.* Ai sensi dell'art. 9, lo Stato membro notificante deve rendere note alla Commissione le informazioni relative al regime di identificazione elettronica e dei relativi livelli di garanzia, al regime di vigilanza ed a quello delle relative responsabilità, al sistema di autenticazione e alle disposizioni relative all'eventuale sospensione o revoca del regime di autenticazione.

Europea[4], nell'ambito degli obiettivi di crescita di Europa 2020, si propone pertanto di garantire il buon funzionamento del mercato interno attraverso un elevato livello di sicurezza e certezza giuridica, affinché i cittadini possano beneficiare ed avvalersi consapevolmente dei servizi elettronici.

2. L'identità digitale e l'identificazione elettronica.

Il Regolamento e-IDAS richiama necessariamente l'attenzione sui temi cruciali dell'identità digitale e dei connessi processi di identificazione elettronica, temi questi che nell'ultimo decennio, sotto l'egida dell'Europa, hanno costituito il "manifesto" delle Agende digitali dei singoli Stati membri.
In una prospettiva sempre più avanguardista, non sembra peregrino poter definire l'identità digitale quale *species* del più generale *genus* dell'identità personale, e ciò con tutte le conseguenze che ne discendono sul piano giuridico.
E' noto che il termine identità deriva dal latino *idem,* "stesso, medesimo", per cui va da sé che l'identità, è un concetto che richiama l'unità della persona, intesa come entità unica e peculiare, cioè proprio quella e non un'altra.
Del pari, l'identità personale, secondo l'impostazione della dottrina tradizionale nonché secondo i generalissimi canoni di matrice costituzionale generalmente riconosciuti, si sostanzia da un lato nel suo nucleo essenziale costituito dal nome e dai contrassegni personali; dall'altro nel diritto del soggetto a vedersi descritto esattamente così come è, cioè senza alterazioni che rivelino all' esterno, alla collettività, una personalità differente o solo appena diversa da quella propria. Non essendo questa la sede per ulteriori approfondimenti, da questi brevi cenni si evince che il tema dell'identità personale, nei termini appena posti, è intrinsecamente e imprescindibilmente connesso con quello della certezza giuridica.
Ciò premesso, entrando ora nel vivo del tema che qui interessa, il concetto di identità digitale[5] rileva sia come oggetto di tutela della identità personale negli ambienti *on-line*, sia come insieme di informazioni digitali che univocamente riconducibili ad un soggetto,

---

[4] "*La Commissione europea ha proposto un'agenda digitale il cui obiettivo principale è sviluppare un mercato unico digitale per condurre l'Europa verso una crescita intelligente, sostenibile e inclusiva",* Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni del 19 maggio 2010, intitolata «*Un'agenda digitale europea*» *COM n. 245.*

[5] A mente dell'art. 1, lett. o) del D.P.C.M. 29 ottobre 2014 "*Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID), nonché dei tempi e delle modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese*", l'identità digitale è stata definita come "*la rappresentazione informatica della corrispondenza biunivoca tra un utente e i suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale secondo le modalità di cui al presente decreto e dei suoi regolamenti attuativi.*" Antologicamente, l'identità digitale è stata definita come "*la rappresentazione virtuale dell'identità reale, che può essere usata durante interazioni elettroniche con persone o macchine*", ERIC NORLIN e ANDRE DURAND in "*Federated Identity Management*", Whitepaper on towards feder- ated identity management, 2002, 4.

fisico o giuridico, consentono l'accesso a servizi e favoriscono relazioni ed interscambi, di natura più o meno istituzionale.
Conseguentemente, l'identificazione elettronica (*electronic identification*) è il processo in seno al quale vengono utilizzati i dati di autenticazione personale (*personal authentication data*) in modalità elettroniche e che, a mente dell'art 3, n. 1 del Regolamento*"rappresentano un'unica persona fisica o giuridica, o un'unica persona fisica che rappresenta una persona giuridica*".
In tale prospettiva, l'identità digitale è al contempo l'insieme ed il risultato delle informazioni e delle risorse concesse da un sistema informatico al suo utilizzatore all'esito di un processo di identificazione, e poiché tali informazioni, tramite la rete *Internet*, possono essere facilmente oggetto di acquisizione e/o manipolazione fraudolenta, ben si comprende il diffuso sentimento di sfiducia che in tali contesti anima i cittadini.
Da qui l'obiettivo della strategia delle istituzioni europee che con il Regolamento hanno inteso dare piena attuazione ai propositi ed ai programmi enunciati nella Digital Agenda for Europe (Maggio 2010), nel piano d'azione sull'*e-Government* 2001-2015 (Dicembre 2010), nel Single Market Act - I e II (rispettivamente Aprile 2011 e Ottobre 2012), nella Road Map per la stabilità e la crescita (Ottobre 2011) ed infine nella proposta di regolamento della Commissione europea del 4 giugno 2012, presupposto del Regolamento in commento. Propositi che, come detto, mirano a creare effettivamente un mercato digitale sicuro e regolamentato da norme comuni e certe.
Come su riferito, dopo l'identificazione si apre la fase del processo di autenticazione e con la quale si mira ad accertare l'identità di una persona fisica o giuridica e l'origine e l'integrità di dati trasmessi elettronicamente e procedere alla verifica e all'eventuale autorizzazione alla fruizione del servizio *on-line* per la cui erogazione la persona procede. Chiaramente, il processo di autentificazione non è privo di criticità anzi, è vero il contrario. Il processo di identificazione complessivamente inteso deve avvenire con l'utilizzo di strumenti tecnologici finalizzati a garantire la sicurezza dell'accesso, quella sicurezza cui ambiscono tutti gli operatori del contesto europeo, siano essi pubblici che privati.

3. I livelli di garanzia

Il fattore sicurezza, nello sviluppo della tecnologia dell'informazione e delle reti di comunicazione di un Paese è un fattore determinante e scatenante. Il concetto di sicurezza in sé è rivelato da indici minimi quali l'autenticità, la disponibilità, l'integrità, il non ripudio e la riservatezza.[6]
Nel sistema che intende definire il Regolamento, un ruolo principe e strategico pertanto è affidato ai c.d. livelli di garanzia per i mezzi di identificazione elettronica rilasciati

[6] Per approfondire il tema sui livelli di sicurezza, *si veda "Cyberterrorismo e Cyberwarfare: profili giuridici e analisi della casistica a livello* internazionale", di F. BOSCO in Diritto dell'Internet, a cura di G. CASSANO, G. SCORZA, G. VACIAGO, pagg. 658, Cedam, Padova, 2013.

nell'ambito di un regime notificato secondo le modalità previste dall'art.9 del Regolamento. I livelli di garanzia costituiscono la cartina tornasole del grado di sicurezza con il quale i mezzi di identificazione elettronica stabiliscono l'identità di una persona. Il livello di garanzia dipende quindi dal grado di sicurezza che i mezzi di identificazione elettronica sono in grado di assicurare.

La volontà di costruire un' identità elettronica con ambizioni transfrontaliere e contemporaneamente "sicura" è stata alla base dei progetti Stork e Stork 2.0 (*Secure identity across borders linked*) – ai quali ha aderito anche l'Italia – i quali hanno posto l'accento, tra l'altro, sui livelli di sicurezza (2, 3 ,4) che dovrebbero essere tenuti per stabilire norme, procedure e requisiti tecnici minimi per i livelli di garanzia *basso, significativo ed elevato.*[7] E proprio i livelli di garanzia **basso, significativo ed elevato** sono quelli individuati dal Regolamento.

Ai sensi dell'articolo 8, il livello di garanzia *basso* fornisce un grado di sicurezza *limitato* relativamente all'identità pretesa o dichiarata di una persona ed è finalizzato ad arginare il rischio di uso abusivo o alterazione d'identità; il livello di garanzia *significativo* fornisce un grado di sicurezza significativo relativamente all'identità pretesa o dichiarata di una persona ed è finalizzato a ridurre *significativamente* il rischio di uso abusivo o alterazione d' identità; ed infine il livello di garanzia *elevato*, in maniera più penetrante rispetto ai livelli precedenti, fornisce un grado di garanzia elevato volto ad impedire l'uso abusivo o alterazione d' identità.

Tali livelli, nello spirito del Regolamento, devono essere chiaramente assicurati a livello comunitario e, nell'ottica dell'interoperabilità, consentono l'accesso a servizi di pari livello ovvero a servizi di livello più basso.

L'art. 8, comma 3, del Regolamento stabilisce che entro il 18 settembre del 2015, la Commissione, attraverso appositi atti esecutivi, dovrà definire specifiche, norme e procedure tecniche minime che specificheranno i livelli nelle tre gradualità, il cui contenuto dipende sostanzialmente dal processo di identificazione e di verifica, dall'attività svolta nonché dai controlli e dai modelli di vigilanza implementati dai singoli Stati membri.

In tale contesto è del tutto evidente che il parametro della sicurezza, indipendentemente dalla sua declinazione, costituisce la *conditio sine qua non* dell'effettiva fruibilità dei servizi *on-line* e che conseguentemente i prestatori di servizi di natura fiduciaria, accreditati e non[8], sono tenuti ad adottare, ai sensi dell'art. 19 del Regolamento, misure tecniche ed organizzative idonee alla gestione tempestiva dei rischi connessi alla sicurezza dei servizi erogati e che in ogni caso dovranno essere conformi, non soltanto al

---

[7] Un altro standard internazionale che rileva in tale contesto, è la norma ISO 29115:2013 che fornisce un quadro regolamentare, articolato in quattro livelli, per la gestione, la mappatura e lo scambio di informazioni relativi all'autenticazione.

[8] A norma dell'art. 22 "*Elenchi di fiducia*", i prestatori dei servizi fiduciari, sono sottoposti almeno ogni 24 mesi e a proprie spese, a verifiche periodiche, da parte di appositi organismi di valutazione di conformità. Su ogni Stato membro incombe l'obbligo di istituire, mantenere e pubblicare appositi elenchi di fiducia, firmati o sigillati elettronicamente in una forma adatta al trattamento automatizzato. Una volta inseriti nelle liste sono riconosciuti in tutti i paesi dell'UE e nei paesi terzi con i quali sono stati conclusi degli accordi.

Regolamento, ma anche agli standard internazionali ETSI e CEN. E proprio in quest'ottica si inserisce una delle novità introdotte dal Regolamento, il Marchio di Fiducia Europeo (Art. 24) - *EU trustmark* - con il quale i fornitori di servizi fiduciari qualificati inclusi negli elenchi tenuti dalle autorità nazionali potranno utilizzare per presentare in modo semplice, riconoscibile e chiaro i servizi fiduciari prestati.

4. Gli *e-Trust services*

Il Regolamento oltre a regolare i processi di identificazione elettronica nei termini sin ora descritti, offre una puntuale ed esaustiva panoramica dei c.d. *e-Trust services*, i servizi fiduciari.

Ai sensi dell'art. 3, n. 16, un *servizio fiduciario* è "*un servizio elettronico fornito normalmente dietro remunerazione e consistente nei seguenti elementi: a) creazione, verifica e convalida delle firme elettroniche, sigilli elettronici o validazioni temporali elettroniche, servizi elettronici di recapito certificato e certificati relativi a tali servizi: oppure b) creazione, verifica e convalida di certificati di autenticazione di siti web; o c)conservazione di firme, sigilli, o certificati elettronici relativi a tali servizi*".

Analogalmente, un "*servizio fiduciario qualificato*" è un servizio di trust che soddisfa i requisiti stabiliti dal Regolamento stesso.

A differenza della Direttiva 1999/93/CEE che si limitava a regolare l'uso delle firme elettroniche e di taluni servizi di certificazione senza nulla disporre in merito agli obblighi di vigilanza dei *service provider*, alle questioni legali e tecniche relative alla interoperabilità transfrontaliera, il Regolamento amplia il perimetro in esame, pionieristicamente tracciato dalla Direttiva, ormai anacronistica e che per questo verrà definitivamente abrogata nel mese di luglio 2016.

Per quanto concerne la disciplina delle Firme elettroniche[9] (FE) - *e-Signature* (artt. 25-34), la Sezione 4 si apre con l'art. 25 il quale fissa il principio in forza del quale alla firma elettronica non possono essere negati effetti giuridici per il solo fatto di essere elettronica o perché non rispetta i requisiti delle Firme Elettroniche Qualificate (FEQ). La FEQ – non anche la Firma Elettronica Avanzata (FEA) – produce gli stessi effetti giuridici di una firma autografa. Conseguentemente un documento firmato elettronicamente[10], qualora la firma elettronica qualificata sia rilasciata da un prestatore di servizi fiduciari qualificato, soddisferà il requisito di forma *ad probationem* godendo della presunzione legale di integrità dei dati in esso contenuti e della relativa origine.

Un importante novità, invece, è l'introduzione del Sigillo elettronico (SE) - *e-Seal* – (artt.

---

[9] Sulle firme elettroniche, diffusamente G. FINOCCHIARO "*Firme elettroniche e firma digitale*", in Diritto dell'Informatica (a cura di) G. FINOCCHIARO E F. DELFINI, pagg. 310, UTET, 2014.

[10] Sul valore del documento informatico, si vede S. BANDERA, in "*Nuove tecnologie della comunicazione e attività della pubblica amministrazione*", in Nuove tecnologie e libertà della comunicazione. Profili costituzionali e profili pubblicistici, (a cura di) M. CUNIMBERTI, pagg. 308, Giuffrè 2008.

35-40), anch'esso, come le FE, nella forma avanzata (SEA) e qualificata (SEQ) garantisce l'origine e l'integrità dei dati di una persona giuridica, indipendentemente dalla firma del legale rappresentante e che pertanto sottende ad una logica diversa dalla *e-Signature* dalla quale, pertanto, va tenuto distinto. Come per la FE, al sigillo elettronico non possono essere negati gli effetti giuridici e l'ammissibilità come prova nei procedimenti giudiziali. Ulteriore elemento di novità rispetto al regime della Direttiva 1999/93/CEE è l'introduzione della *"Validazione Temporale Elettronica"* (Art. 41) che è funzionalmente preordinata ad attestare il momento a partire dal quale il documento può dirsi validamente formato. Sostanzialmente è il *dies a quo* dal quale decorrono i termini ai fini di determinati effetti giuridici.

Le novità non finiscono qui. Il Regolamento infatti introduce il Servizio Elettronico di Recapito Certificato (Art. 43) la cui disciplina, quanto agli effetti , è sostanzialmente uguale a quella vista per le firme ed i sigilli elettronici. Si tratta di un servizio che consente la trasmissione di dati fra terzi per via elettronica e fornisce prove relative al trattamento dei dati trasmessi, fra cui prove dell'avvenuto invio e dell'avvenuta ricezione dei dati, e protegge i dati trasmessi dal rischio di perdita, furto, danni o di modifiche non autorizzate. In via del tutto analoga, il Servizio Elettronico di Recapito Qualificato Certificato è un servizio elettronico di recapito certificato erogato da prestatori di servizi fiduciari e che soddisfa i requisiti richiesti dall'art. 44 del Regolamento.

Infine, il Regolamento prescrive disposizioni relative ai requisiti che i certificati qualificati per l'autenticazione di siti web (Art. 45), devono possedere, rinviando per la normativa di all'Allegato IV[11] e ribadisce il concetto di neutralità tecnologica in relazione agli "*Effetti giuridici dei documenti elettronici*" (Art. 46). nella misura in cui il documento elettronico non può essere privato in sede giudiziale degli effetti giuridici che gli sono propri.

Anche da quest'ultima norma passata in rassegna, emerge con tutta evidenza che il Regolamento e-IDAS è fortemente orientato alla promozione del principio della neutralità

---

[11] *"I certificati qualificati di autenticazione di siti web contengono :a) un'indicazione, almeno in una forma adatta al trattamento automatizzato, del fatto che il certificato è stato rilasciato quale certificato qualificato di autenticazione di sito web; b) un insieme di dati che un insieme di dati che rappresenta in modo univoco il prestatore di servizi fiduciari qualificato che rilascia i certificati qualificati e include almeno lo Stato membro in cui tale prestatore è stabilito e — per una persona giuridica: il nome e, se del caso, il numero di registrazione quali appaiono nei documenti ufficiali, — per una persona fisica: il nome della persona; c) per le persone fisiche: almeno il nome della persona a cui è stato rilasciato il certificato, o uno pseudonimo. Qualora sia usato uno pseudonimo, ciò è chiaramente indicato; per le persone giuridiche: almeno il nome della persona giuridica cui è stato rilasciato il certificato e, se del caso, il numero di registrazione quali appaiono nei documenti ufficiali; d) elementi dell'indirizzo, fra cui almeno la città e lo Stato, della persona fisica o giuridica cui è rilasciato il certificato e, se del caso, quali appaiono nei documenti ufficiali; e) il nome del dominio o dei domini gestiti dalla persona fisica o giuridica cui è rilasciato il certificato; f) l'indicazione dell'inizio e della fine del periodo di validità del certificato; g) il codice di identità del certificato che deve essere unico per il prestatore di servizi fiduciari qualificato; h) la firma elettronica avanzata o il sigillo elettronico avanzato del prestatore di servizi fiduciari qualificato che rilascia il certificato; i) il luogo in cui il certificato relativo alla firma elettronica avanzata o al sigillo elettronico avanzato di cui alla lettera h) è disponibile gratuitamente; j) l'ubicazione dei servizi competenti per lo status di validità del certificato a cui ci si può rivolgere per informarsi sulla validità dei certificato qualificato".*

tecnologica[12] in ragione del quale ad un documento elettronico non devono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica.

5. Il Regolamento e-IDAS e il sistema italiano SPID: un confronto

Dall'analisi sin qui svolta, il Regolamento e-IDAS non sembra particolarmente differire dal quadro giuridico italiano disegnato dal D.Lgs. 7 marzo 2005, n. 82 s.m.i. ("*Codice dell'Amministrazione Digitale*" C.A.D.) Invero, in attuazione dell'articolo 64, comma 2-*sexies* del C.A.D., è stato pubblicato in Gazzetta Ufficiale n. 285 del 9 dicembre 2014, il D.P.C.M. del 24 ottobre 2014 "*Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID), nonché dei tempi e delle modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese*", (di seguito, "Decreto SPID").
Tale Decreto, in attuazione altresì dell'art. 17-*ter* del Dlgs. 21 giugno 2013, n. 69, (convertito con L. 9 agosto 2013, n. 98) c.d. "*Decreto del Fare*", prevede che il Sistema SPID, "*costituito come insieme aperto di soggetti pubblici e privati che, previo accreditamento da parte dell'Agenzia per l'Italia Digitale, gestiscono i servizi di registrazione e di messa a disposizione delle credenziali e degli strumenti di accesso in rete nei riguardi di cittadini e imprese per conto delle pubbliche amministrazioni*" prenderà avvio verosimilmente nel mese di Aprile 2015.
I soggetti che parteciperanno allo SPID sono dunque i gestori dell'identità digitale, i gestori degli attributi qualificati, i fornitori di servizi, l'Agenzia per l'Italia Digitale[13] – AgID

---

[12] Sul principio di neutralità tecnologica, G.Finocchiaro, *op. cit.*, pagg. 64. Con riguardo ai servizi di comunicazione elettronica, come ha avuto modo di affermare certa dottrina, "*il principio di neutralità è declinato nelle proposte avanzate come neutralità tecnologica e neutralità nei confronti del servizio (…) va interpretato come la necessità di ridurre la massimo le restrizioni nell'uso delle tecnologie per la fornitura di un servizio di comunicazione elettronica",* M.Orofino, in "*Profili costituzionali delle comunicazioni elettroniche nell'ordinamento multilivello"*, pagg. 236, Giuffrè 2008.

[13] Istituita con D.L. n. 83/2012, convertito nella L. 134/2012 ed è sottoposta ai poteri di indirizzo e vigilanza del Presidente del Consiglio dei Ministri o del Ministro da lui delegato. In forza dell'articolo 4 del Decreto SPID, "1. *L'Agenzia cura l'attivazione dello SPID, svolgendo, in particolare, le seguenti attività: a) gestisce l'accreditamento dei gestori dell'identità digitale e dei gestori di attributi qualificati, stipulando con essi apposite convenzioni. Con i regolamenti di cui al presente articolo sono disciplinate le convenzioni per l'adesione allo SPID da parte dei fornitori di servizi ed è regolato il contributo che i gestori dell'identità digitale accreditati allo SPID riconoscono all'Agenzia, da determinarsi nella misura necessaria alla copertura dei costi sostenuti da quest'ultima; b) cura l'aggiornamento del registro SPID e vigila sull'operato dei soggetti che partecipano allo SPID, anche con possibilità di conoscere, tramite il gestore dell'identità digitale, i dati identificativi dell'utente e verificare le modalità con cui le identità digitali sono state rilasciate e utilizzate; c) stipula apposite convenzioni con i soggetti che attestano la validità degli attributi identificativi e consentono la verifica dei documenti di identità. A tali conven-*

– e gli utenti. I soggetti pertanto sono gli stessi, con le dovute differenziazioni, previsti dal Regolamento.
Con il sistema SPID gli utenti potranno far ricorso a gestori di identità digitale e di gestori di attributi qualificati, per consentire ai fornitori di servizi l'immediata verifica della propria identità e degli eventuali attributi qualificati connessi e ciò al fine di accedere in maniera sicura ed immediata ai servizi erogati *on-line* dalle Pubbliche Amministrazioni.
Si tratta di un progetto di *e-governament* ambizioso ed altamente innovativo che, senza sovrapporsi, si pone in piena sintonia con il Regolamento. Nel Regolamento infatti sono stabiliti dei requisiti minimi comuni e l'Italia, con lo SPID, li rispetta pienamente. Ogni Stato membro al fine di osservare le prescrizioni del Regolamento – obbligatorio in tutti i suoi elementi – dovrà fare altrettanto predisponendo un proprio sistema di identità neutro ed interoperabile con i sistemi di identità degli altri Sati membri.
Grazie al Sistema SPID e al Regolamento, l'identità digitale in Italia, è destinata a conoscere un forte cambiamento.
Anzitutto il Decreto SPID prevede una serie di tappe scandite temporalmente che conducono, come detto, verosimilmente entro il mese di aprile 2015, all'accreditamento del primo *Identity Provider*: a partire da tale evento, a mente dell'art. 14 del Decreto SPID, tutte le Pubbliche Amministrazioni Italiane avranno tempo 24 mesi per accreditarsi presso l'AgID.
Entro 24 mesi pertanto, le Pubbliche Amministrazioni dovranno mettere i cittadini nelle condizioni di poter richiedere ed accedere ai servizi *on-line* mediante l'utilizzo della propria identità digitale, così come previsto dall'art. 64 comma 2 del C.A.D., così come modificato dall'art. 17-*ter* del Decreto del Fare.
Allo stesso modo l'AgId ha ventiquattro mesi per individuare le precise modalità con le quali le varie tipologie di PA potranno iniziare a usare SPID e questa è la che attende l'Agenzia e il suo Comitato di Indirizzo.[14]
Anche dal punto di vista dei livelli di sicurezza, il Sistema SPID si pone in piena conformità a quanto richiesto dal Regolamento tanto dal punto di vista della neutralità tecnologica tanto da quello della sicurezza. L'art. 6 del Decreto SPID, prevede infatti che il Sistema SPID si basa su tre livelli di sicurezza di autenticazione informatica (Level of Assurance), LoA2 dello standard ISO/IEC DIS 29115 (basso), LoA3 dello standard ISO/IEC DIS 29115 (significativo) e LoA4 dello standard ISO/IEC DIS 29115 (elevato): spetterà all'AgID valutare e autorizzare l'uso degli strumenti e delle tecnologie di autenticazione informatica consentiti per ciascun livello.
Insomma, da queste prime considerazioni dalla pubblicazione in Gazzetta Ufficiale del Decreto SPID, emerge con tutta evidenza che il Sistema SPID ha risposto più che bene

zioni i gestori dell'identità digitale e i gestori degli attributi qualificati sono tenuti ad aderire secondo le modalità indicate nei regolamenti di cui al presente articolo".

[14] Un attenta e recente analisi delle prospettive e delle imminenti sfide legate all'identità digitale e ai servizi erogati dalle Pubbliche Amministrazioni nell'ambito del Sistema SPID, è offerta da E.PROSPERETTI nel suo articolo dal titolo "*Il 2015 dell'identità digitale*", su "Agenda Digitale.eu", consultabile all'indirizzo http://www.agendadigitale.eu/identita-digitale/1240_l-identita-digitale-passa-alla-fase-esecutiva-ecco-come-sara.htm.

ed in fretta al legislatore europeo, ponendo sin da subito le basi per la creazione di un sistema di autenticazione fruibile e sicuro e idoneo ad accelerare lo scambio di domanda ed offerta dei servizi pubblici digitali.

6. Conclusioni

Dalle considerazioni sin qui svolte è evidente che i temi legati all'e-Identity impegneranno considerevolmente il dibattito dei prossimi anni, soprattutto alla luce della rilevanza che l'identità digitale delle persone e delle imprese, con tutte le implicazioni che porta con sé, ricopre per lo sviluppo economico, civile e sociale di un Paese. Se per un verso l'identità digitale è un fattore abilitante, che consente l'accesso a numerosi servizi, dall'altro costituisce un fattore di rischio per la tutela dell'individuo. Da qui l'esigenza di costruire un'identità digitale, individuale e collettiva, affidabile e sicura. E' proprio in tale contesto che si inserisce il Regolamento, che persegue l'obiettivo di istituire un quadro normativo uniforme, volto a promuovere l'interoperabilità, sviluppare la cittadinanza digitale e prevenire la criminalità cibernetica. Un modello unico insomma al quale l'Italia, nell'ambizioso quanto non facile progetto di costituzione di un'identità digitale europea, sembra volervi convergere velocemente.

N. 3 - 2015 · pp. 37-50

La tutela della privacy dei minori: gli strumenti self-regulation dell'Unione Europea

Fabrizio Corona

Abstract: L'area di protezione della privacy dei bambini su Internet ha recentemente assistito ad un numero di sviluppi di self-regulation (autoregolamentazione) nell'UE. Oltre ai principi Safer Social Networking ed il codice FEDMA, di recente i due ICT e CEO coalitions hanno adottato i principi relativi alla sicurezza dei bambini e della privacy online. Questi quattro strumenti del settore privato hanno come obiettivo di mitigare i rischi della privacy online, come l'uso improprio di dati personali, lo sfruttamento commerciale dei dati ed i rischi.Anche se gli organi dell'UE considerano gli strumenti di self-regulation come strumenti altamente promettenti, la loro attuazione e la loro efficacia son discutibili. Basato su un approccio concettuale per valutare strumenti normativi alternativi, sviluppato da Latzer, questo documento valuta come efficacemente i quattro strumenti di regolamentazione funzionano per quanto riguarda il loro obiettivo di proteggere i bambini dai rischi della privacy online.

The area of children's privacy protection on the Internet has recently witnessed an increased number of self-regulation developments in the EU. Besides the Safer Social Networking Principles for the EU, the FEDMA Code and recently two self-regulation ICT industry-led Coalitions (ICT and CEO coalitions) adopted principles related to children's safety and privacy online. In these four instruments private industry actors aim, among other goals, to mitigate online privacy risks, such as personal data misuse, commercial data exploitation, conduct and contact risks.Although EU policy makers and the industry consider self-regulation instruments as highly promising tools, their implementation among companies, as well as their durability and effectiveness are questionable. Based on a conceptual approach to evaluate alternative regulatory instruments, developed by Latzer, this paper evaluates how effectively the four aforementioned self-regulation schemes function as regards one of their aims to protect children from online privacy risks.

Parole Chiave: self-regulation, privacy, minore, internet, sicurezza, Unione Europea

Articolo pervenuto il 10 febbraio 2015, approvato il 20 febbraio 2015

regulation – 4.2.L'azione degli strumenti di self-regulation – 4.2.1.Monitoraggio – 4.2.2. Reclami e Controversie – 4.2.3.Sanzioni – 4.3.L'intervento del diritto sugli strumenti self-regulation – 5.Riflessioni conclusive

1. Introduzione

L'area di tutela della privacy dei minori su Internet, ha recentemente assistito ad un notevole aumento di attenzione e regolamentazione da parte dell'Unione Europea. I principali fattori trainanti di questo interesse, sono la crescente importanza dei diritti del minore, compreso il diritto alla protezione dei dati personali, e le preoccupazioni relative alla loro sicurezza online. Quest'ultimo fattore è emerso come una risposta ad un forte aumento dell'utilizzo di Internet da parte di bambini sempre più piccoli. La tutela della privacy e dei dati personali in tale ambiente è diventato un requisito indispensabile per garantire la sicurezza dei minori online.
Anche se i diritti dei bambini alla privacy ed alla tutela dei dati personali sono diritti umani fondamentali e quindi la tutela della privacy dovrebbe costituire un interesse pubblico, la sua regolamentazione, invece, è sempre passata nelle mani di attori privati. Negli ultimi anni, un insieme di soggetti legati al settore dell'ICT, si sono attivamente impegnati per concordare strumenti di autoregolamentazione (self-regulation) sul fronte della sicurezza dei bambini, tra cui la privacy e la protezione su Internet. La Commissione Europea ha svolto un ruolo significativo nel facilitare, piuttosto che dominare, questo processo normativo. Come risultato di questo processo, l'industria di Internet ha adottato diversi codici volontari di condotta, linee guida e principi. Gli sviluppi normativi concreti sono: i Principi Safer Social Network per l'Unione Europea, ossia una disposizione regolamentare tra i fornitori di servizi di social networking, il codice FEDMA, codice europeo di condotta e di autodisciplina per l'uso di dati personali nelle attività di direct marketing e le ICT e CEO coalitions dove sono stati stabiliti i principi relativi alla sicurezza ed alla privacy online dei bambini.
Questi quattro strumenti, tra gli altri obiettivi, mirano a mitigare i rischi per la privacy online, come l'uso improprio di dati personali, lo sfruttamento commerciale di tali dati ed i rischi connessi al loro utilizzo improprio. Benché il processo di autoregolamentazione e regolamentazione privata è stato presentato dalla Commissione Europea come pietra miliare nel processo di regolamentazione della tutela dei minori online, l'efficacia di tale tutela diventa fondamentale al fine di garantire una protezione effettiva. Nonostante l'evidente vantaggio che porta la soft law, come le competenze socio-tecnologiche del settore, l'innovazione, la velocità di reazione e di riduzione dei costi degli enti pubblici, è ancora percepita come una regolazione intrinsecamente debole o inefficace. Gli studiosi temono che la autoregolamentazione, come base comunitaria per la regolamentazione privata, pone problemi di legittimità, per le sue significative differenze rispetto al tradizionale modello democratico. Se la regolamentazione privata determina un implementazione tecnica di autorità, c'è da chiedersi fino a che punto essa può avanzare un contrasto tra i

vari interessi pubblici e privati[1]. Non sorprende, quindi, che per bilanciare il rapporto tra gli interessi pubblici e privati nel processo di regolamentazione, l'Unione Europea abbia, col tempo, dato una maggiore attenzione al sistema di co-regolamentazione che, a causa delle diverse forme che può assumere, non garantisce sempre il suo risultato normativo.

2. L'Online Privacy Risk

Il problema che attualmente viviamo, è che dovrebbe essere in parte mitigato da un sistema di self-regolation, riguarda la questione di come proteggere i minori. Per inquadrare tale problema, è necessario capire il significato del termine *"online privacy risk"*.
Il termine on-line indica, a prima vista, una realtà virtuale dove gli utenti internet svolgono le loro attività, come ad esempio il consumo o la creazione di contenuti online. Tuttavia, per apprezzare le varie dimensioni di questo termine in relazione alle attività dei bambini online, è necessario tener presente che i bambini accedono ad internet mediante piattaforme sempre differenti e non sempre con PC desktop tradizionalmente utilizzati a casa o scuola. Sono sempre più frequenti smartphone ed altri dispositivi elettronici che sono diventati sempre più popolari in bambini sempre più piccoli.
Il rischio è un concetto complesso. Anche se generalmente inteso come *"possibilità di perdita o pregiudizio",* o *"una fonte di pericolo"*[2] non esiste una definizione universalmente riconosciuta di rischio. Le ragioni sono molteplici; in primo luogo, la comprensione di quali azioni sono a rischio ha forma diversa a seconda della cultura e della società. Come notato da Staksrud, molti fattori collettivi, come il sistema d'istruzione, i valori culturali o il quadro normativo, stabiliscono cosa possa essere percepito come pericolo dalle persone o dalle Nazioni.[3] Ad esempio, per quanto riguarda le attività dei bambini online, la loro percezione delle attività pericolose in internet, può essere dettato dall'influenza dei genitori degli insegnanti o dai stessi compagni di scuola. In secondo luogo la percezione, a livello individuale di un'attività rischiosa è spesso molto soggettiva, in quanto dipende dalla propria esperienza di vita.
Quando si tratta di bambini e del loro comportamento online, i dibattiti in materia sono dominati dall'immagine del bambino come vittima impotente o utente vulnerabile. L'uso di Internet da parte dei bambini è più visto come qualcosa creazione di un rischio o pericolo, piuttosto che fornire opportunità positive. Importante notare che il rischio si riferisce alla possibilità di un pericolo, che non necessariamente avviene o si traduce in un danno. La ricerca EU kids Online ha dimostrato che non tutti i bambini che erano coinvolti in comportamenti a rischio sulla rete hanno subito un danno. Situazioni di rischio possono provocare non solo conseguenze dannose ma possono temprare il carattere

---

1 Colin Scott, *Beyond Taxonomies of Private Authority in Transnational Regulation*, p. 1330.

2 Elisabeth Staksrud, *Children in the Online World: Risk, Regulation, Rights.* London:Ashgate, 2013, p. 53

3 Elisabeth Staksrud, *Children in the Online World: Risk, Regulation, Rights.* London:Ashgate, 2013, p. 53

e fargli acquisire maggiore resistenza e consapevolezza dei rischi sulla rete[4]. È utopico poter pensare di eliminare tutti i rischi e pericoli che la rete possa procurare ai minori che navigano, ma è opportuno garantire una responsabilizzazione degli utenti di Internet. La privacy non è un concetto di certo meno complesso di quello di rischio. Nonostante un ampio dibattito tra filosofi, sociologi e tecnici del diritto, è ancora difficile cogliere il significato di questo concetto. L'idea di privacy come *"the right to be left alone"* coniato da Waren e Brandeis[5] implica il desiderio di agire in una zona privata, che è fuori dal controllo del pubblico. Un approccio simile proviene da Westin, che ha definito la privacy come *"la pretesa di individui, gruppi, istituzioni di determinare per se stessi, come e in che misura le informazioni su di loro vengono comunicate agli altri"*[6]. Infine un'altra definizione è stata data da Helen Nisenbaum che definisce la privacy come *un "concetto sociale ed è relativo al rispetto dei limiti contestuali entro cui informazioni personali vengono condivise"*[7].
Dato questo contesto, possiamo definire "online priacy risk" la possibilità di perdita di privacy nel mondo offline a causa di attività online.

3. La tutela della privacy online dei minori in Europa come oggetto di self-regulation

Il ricorso alla self-regulation, piuttosto che alla legislazione, per tutelare la sicurezza e la privacy dei bambini online in Europa può essere fatta risalire alla metà degli anni '90. Da allora le politiche per creare un Internet più sicuro per i bambini hanno posto l'accento su strumenti normativi alternativi, come il self-regulation e la co-regulation. La preferenza per gli strumenti di self-regulation è stato recentemente confermato nella comunicazione "Strategy for a Better Internet for Children" del maggio 2012, dove si è dichiarato che *"la legislazione non verrà scartata, ma verrà data preferenza al sistema self-regulation, che resta più flessibile per conseguire risultati tangibili in questo campo"*[8].
Analogamente l'agenda digitale per l'Europa comporta l'obiettivo di promuovere il dialogo multi – stakeholder e di self-regulation tra i fornitori di servizi europei e mondiali, come ad esempio i social network, i fornitori di comunicazioni mobili.

---

4 L Hasebrink, Uwe, Livingstone, Sonia and Haddon, Leslie (2008) *Comparing children's online opportunities and risks across Europe: cross-national comparisons for EU Kids Online.* EU Kids Online, Deliverable D3.2. EU Kids Online Network, London, UK

5 Samuel Warren, Louis Brandeis, The Right to Privacy. *Harvard Law Review*, Vol. 4 (5), 1890.

6 Alan F. Westin, *Privacy and freedom*. 1st ed. New York: Atheneum, 1967, p. 7

7 Helen Nissenbaum, Helen, Privacy as contextual integrity. Washington Law Review, Vol. 79 (119), 119-159, 2004.

8 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions European Strategy for a Better Internet for Children, COM (2012) 196 Final, p. 6.

Attualmente esistenti per la privacy dei minori in internet ci sono le quattro iniziative elencate nell'introduzione del presente articolo.Tre dei quattro strumenti regolamentano la sicurezza della privacy online del bambino, con principi molto simili tra loro. Il quarto strumento, il FEDMA, è utilizzato per il sistema della pubblicità online e dedica una parte alla tutela della privacy del minore nel caso di utilizzo improprio di dati personali per finalità commerciali.

3.1. Safer Social Networking Principles

Il Safer Social Networking Principles per l'Unione Europea è uno dei primi esempi di autoregolamentazione nel settore di sicurezza online dei minori.Avviato e sostenuto dalla Commissione Europea, questo self-regulation riunisce circa 20 servizi di social networking (SNS). Il documento delinea i sette principi dai quali i fornitori di SNS dovrebbero essere guidati che cercano di minimizzare il danno potenziale per i bambini ed i giovani e raccomanda una serie di buone pratiche e di approcci che possono contribuire al raggiungimento di tali principi.
Il primo principio si *intitola "Aumentare la consapevolezza dei messaggi di educazione alla sicurezza e le policy di utilizzo accettabile per gli utenti, genitori, insegnanti e accompagnatori in un modo chiaro ed appropriato all'età".* Con questo principio, i fornitori dovrebbero creare materiali didattici progettati per dare ai bambini ed ai giovani gli strumenti, conoscenze e competenza per navigare in modo sicuro. I messaggi devono essere presentati in un formato facile e pratico per essere compresi ed inoltre compito dei fornitori del servizio è di offrire ai genitori collegamenti mirati, materiale ed altri controlli tecnici mirati a favorire il dialogo, la fiducia ed il coinvolgimento tra genitori e figli sull'uso responsabile di Internet.
Il secondo principio, dal titolo *"Adoperarsi per garantire che i servizi siano adatti alla loro età per i destinatari"*, si stabilisce che i fornitori dovrebbero, nel normale corso di sviluppo e gestione SNS, considerare come il loro servizio può essere associato a potenziali rischi per i bambini ed i giovani. Il fornitore deve limitare l'esposizione potenzialmente pericolosa a contenuti non adatti, rendendo chiari quando i servizi non sono adatti per i bambini ed i giovani o dove è necessario l'età minima per la registrazione, adottare misure per identificare ed eliminare gli utenti minorenni dai loro servizi, adottare misure per impedire agli utenti di tentare di registrarsi nuovamente con un età diversa oppure promuovendo l'adozione del parental control.
Nel terzo principio intitolato *"consentire agli utenti attraverso strumenti e tecnologie"*, i fornitori dovrebbero utilizzare strumenti e tecnologie per aiutare i bambini ed i giovani nella gestione del servizio, in particolare per quanto riguarda contenuti inappropriati. Le misure da adottare consentono di ridurre al minimo il rischio di contatti indesiderati o inappropriati per il minore, come ad esempio assicurando che il profilo del minore possa essere visualizzato solo dagli utenti appartenenti alla lista amici, o garantendo l'accesso alla lista amici di soli utenti con un età inferiore ai 18 anni.
Il quarto principio, dal titolo *"Fornire facili strumenti per segnalare comportamenti o contenuti che violano le condizioni di servizio",* i fornitori dovrebbero fornire un

meccanismo per segnalare i contenuti inappropriati, contatti o comportamenti come indicati nelle loro condizioni generali di servizio. Tale meccanismo deve essere facilmente accessibile agli utenti in qualsiasi momento e la procedura deve essere facilmente comprensibile.
Il quinto principio si intitola *"rispondere alle notifiche di contenuto illegale o di condotta"*. Al ricevimento della notifica di presunti contenuti o comportamenti illeciti, i fornitori dovrebbero avere un sistema per consentire la rimozione immediata del contenuto offensivo.
Il sesto principio, dal titolo *"Abilitare e incoraggiare gli utenti ad assumere un approccio sicuro alle informazioni personali ed alla vita privata"*, i fornitori dovrebbero fornire una gamma di opzioni di impostazione di privacy con le informazioni di supporto che incoraggi gli utenti a prendere decisioni circa le informazioni che decidono di pubblicare. Queste opzioni dovrebbero essere accessibili facilmente ed in qualsiasi momento.
Il settimo ed ultimo principio, dal titolo *"Valutare i mezzi per esaminare contenuti illegali o proibiti",* impone ai fornitori di SNS di valutare il loro servizio per identificare potenziali rischi per i bambini ed i giovani al fine di determinare adeguate procedure per la revisione e segnalazione di immagini, video e contenuti illeciti.

3.2 CEO Coalition, per far diventare internet un posto migliore per il minore

Il CEO Coalition per far diventare internet un posto migliore per il minore, è stato progettato per raccogliere una vasta gamma di aziende private che lavorano nei vari settori della ICT (produttori di cellulari, fornitori di sistemi, Internet service provider). Il progetto è stato lanciato dal vice presidente del Parlamento Europeo e Commissario Europeo per l'agenda digitale Neelie Kroes. In tale progetto è stato previsto di proporre e sviluppare soluzioni e misure per rendere Internet un "luogo più sicuro per i bambini". Le aree in cui le società hanno deciso di agire e sviluppare soluzioni sono: strumenti semplici per gli utenti di segnalare contenuti dannosi e contatti, impostazioni privacy adeguate all'età, un uso più ampio di classificazione dei contenuti, una più ampia disponibilità e l'uso di controlli parentali, il controllo di materiale pedopornografico.
A partire da gennaio 2014, 31 aziende hanno aderito al CEO Coalition. Il funzionamento della sistema si è basato su diverse forme di incontro e gruppi di lavoro: riunioni di società, riunioni di settore di attività ed incontri aperti a tutte le parti interessate.[9]
Lo stato attuale della Coalizione non è molto chiaro. Dopo il primo anno di funzionamento il progetto è stato sospeso, anche se pubblicamente i membri della Coalizione e la Commissione Europea hanno affermato il loro impegno a collaborare.

[9] The CEO Coalition (2011) "Coalition to make the Internet a better place for kids: statement purpose" Retrieved 2012 07 30, from http://ec.europa.eu/information_society/activities/sip/docs/ceo_coalition/ceo_coalition_statement.pdf Annex I.f

3.3 ICT Coalition, per l'uso sicuro dei dispositivi collegati a servizi online dei bambini e giovani nella UE

Un altro simile, identico nelle sue finalità al CEO Coalition, è l'ICT Coalition. Poco prima del lancio della CEO Coalition, il settore ICT aveva realizzato una coalizione realizzando una serie di principi analoghi.

Nel primo principio, denominato *"Content"*, stabilisce che alcuni contenuti online potrebbero non essere adatti per i bambini ed i giovani. I firmatari dovrebbero pertanto: indicare chiaramente dove un servizio che offrono possa includere contenuti non considerati adatti per i bambini ed in maniera visibile opzioni che sono disponibili per il controllo dell'accesso al contenuto. Questo potrebbe includere, per il servizio, strumenti per gestire l'accesso a determinati contenuti, consulenza agli utenti o di un sistema riconosciuto di contenuti. Visualizzare in una posizione facilmente accessibile la Politica d'Uso Accettabile, che dovrebbe essere scritta in un linguaggio facilmente comprensibile. Indicare chiaramente qualsiasi modifica ai termini di servizio o di orientamenti comunitari (vale a dire come gli utenti dovrebbero comportarsi e ciò che non è accettabile) con cui contenuti generati dagli utenti devono uniformarsi. Assicurarsi che le opzioni di reporting siano nei settori pertinenti del servizio. Fornire avviso circa le conseguenze per gli utenti che nel postare contenuti non rispettino termini di servizio o normative comunitarie. Proseguire i lavori per fornire soluzioni innovative in grado di supportare la protezione di sicurezza per bambini con strumenti e soluzioni.

Nel secondo principio, dal titolo *"Parental Control"*, si stabilisce che i firmatari dovrebbero aiutare i genitori a limitare l'esposizione dei bambini ai contenuti potenzialmente inappropriati.

Nel terzo principio, denominato *"dealing with abuse/misuse",* si stabilisce che dove i contenuti o la condotta possa essere illegale, dannosa od offensiva, i firmatari dovrebbero fornire un processo chiaro e semplice on cui gli utenti possono segnalare contenuti o comportamenti che violino le condizioni del servizio. Implementare procedure appropriate per la segnalazione degli utenti circa immagini, video ed altri contenuti inappropriati e fornire agli utenti informazioni chiare per le eventuali procedure di revisione dei contenuti.

Nel quarto principio, *"Child abuse or illegal contact"* si stabilisce che i firmatari in caso di abuso sessuale infantile, come immagini di abusi sessuali distribuiti su internet, devono cooperare con le autorità incaricate dell'applicazione della legge, come previsto dalla legge locale e garantire la pronta rimozione di contenuti illegali contenenti le immagini con l'abuso.

Nel quinto principio *"Privacy and Control"* si stabilisce che i firmatari rispetteranno la protezione dei dati esistenti e la tutela della privacy come stabilito dalle disposizioni di legge. Inoltre, a seconda dei casi, i firmatari dovranno gestire le impostazioni di privacy appropriate per i bambini e per i giovani in modo da garantire una quanto più maggiore tutela. Offrire una gamma di opzioni di impostazione di privacy che incoraggino i genitori, bambini e giovani a prendere le decisioni informate sul loro uso del servizio, adottare

misure, se del caso e conformemente agli obblighi di legge, per informare l'utente dei diversi controlli della privacy che sono abilitati ed infine fare lo sforzo per aumentare la consapevolezza tra tutte le parti in relazione alla protezione dei bambini e dei giovani sulla rete.
Nel sesto ed ultimo principio, *"education and awareness",* i firmatari si impegnano a fornire informazioni appropriate ed impegnarsi in attività di sensibilizzazione per l'uso dei dispositivi collegati online. Lo scopo di queste attività sarà di educare i bambini ed i giovani a dare loro informazioni aggiornate per la gestione del loro accesso e le impostazioni relative ai contenuti. Fornire consigli sulle funzionalità del servizio o funzionalità che sono disponibili per consentire ai genitori la migliore protezione del minore.
Tali aree di interesse si sovrappongono con quelle della CEO Coalition. Con tali principi si obbliga una società, o gruppo di imprese, a presentare una bozza di documenti, che afferma quali obiettivi si vogliono raggiungere ed i parametri di riferimento. Le società firmatarie di questa iniziativa, sono tenute a riferire sui loro progressi in 18 mesi dopo l'adozione dei principi.

3.4 FEDMA – Federazione europea del direct marketing

Nel 2003, la federazione europea del direct marketing ha adottato il codice europeo di condotta e di autodisciplina per l'uso di dati personali nelle attività di direct marketing. Più recentemente, nel 2010, a seguito di un ampio processo di consultazione, il codice è stato integrato con un allegato che ha aggiunto alcune disposizioni. In particolare, la Sezione 6 del codice si occupa delle "disposizioni particolari relative al Minore", dove si stabilisce che nel raccogliere dati di minori, il responsabile del trattamento dei dati dovrà sempre fare ogni ragionevole sforzo affinché il minore e/o genitore siano opportunamente informati dagli scopi del trattamento dati del minore. In particolare, nell'utilizzare materiale commerciale rivolto ai minori, o altrimenti nel raccogliere consapevolmente dati da minori, l'informativa dovrà essere posta in evidenza ed essere facilmente accessibile e comprensibile al minore.
Ove la legge nazionale o europea sulla protezione dei dati preveda in consenso dell'Interessato al trattamento, il responsabile del trattamento dei dati dovrà ottenere il consenso informato e preventivo dal genitore del minore.
Inoltre il responsabile del trattamento dei dati dovrà fare ogni ragionevole sforzo per verificare che la persona che esercita il diritto del minore sia il genitore. Lo stesso responsabile non dovrà condizionare la partecipazione del minore ad un gioco, all'offerta di un premio o a qualsiasi altra attività che comporti un vantaggio promozionale al fatto che il minore divulghi più dati personali di quanti non siano strettamente necessari per partecipare all'attività.

4. Il sistema Latzer per l'analisi degli strumenti di self-regulation

Dopo aver descritto gli strumenti self-regulation adottati all'interno dell'Unione Europea per la tutela della privacy dei minori su Internet, analizziamo se ed in che misura tali strumenti abbiano realizzato i loro obiettivi. Per conoscere bene i quattro strumenti di self-segulation, quale impatto hanno e se essi contribuiscono al raggiungimento complessivo dell'obiettivo pubblico di proteggere i minori dai rischi online, è necessario scegliere adeguati indicatori di valutazione.
L'approccio più completo per valutare sistematicamente il funzionamento dei sistemi di self-regulation è stato sviluppato da Latzer nel 2007[10]. Tale approccio di valutazione tiene conto di fattori organizzativi ed istituzionali che spiegano il livello delle prestazioni alternative di regolamentazione. Tale metodo si sviluppa sull'analisi ex ante ed ex post dei sistemi di regolamentazione; nella fase ex ante si prevede la fattibilità e l'efficacia degli strumenti di self-regulation, mentre nella fase ex post si valuta la perfomance degli strumenti adottati.
Tale sistema valutativo si basa sul presupposto che le prestazioni di qualsiasi strumento di self-regulation è determinato da quattro fattori: l'adozione, la consapevolezza, l'atteggiamento e l'azione. In aggiunta a tali fattori si deve considerare la particolare struttura dell'ente regolatore (fattori istituzionali/organizzativi) e dalle specifiche di mercato, ambiente ed i regolamenti (fattori contestuali). I fattori istituzionali/organizzativi sono flessibili e possono essere modificati a livello organizzativo. Essi comprendono la chiara definizione degli obiettivi, gli standard da adottare per gli strumenti di self-regulation sanzioni adeguate, periodici, revisioni esterne. Al contrario, i fattori contestuali possono essere modificati solo con la riforma di tutto il contesto normativo.
Tali fattori servono per comprendere il funzionamento di sistemi di self-regulation. Per analizzare l'impatto che tali strumenti hanno avuto nel panorama europeo, faremo riferimento ai criteri di azione e di adozione.

4.1 L'adozione degli strumenti di self-regulation

Come notato da Bonnici, una delle principali caratteristiche degli strumenti di salf-regulation è che le regole *"siano sviluppate ed accettate da coloro che prendono parte a una attività"*[11]. Ciò significa che i soggetti privati devono tra loro riconoscere la necessità di regolamentare un determinato problema e di tradurre questa esigenza in una regola reciprocamente accettata. Nel contesto dei quattro strumenti oggetto di analisi, possiamo

[10] Michael Latzer, Monroe E. Price, Florian Saurwein, Stefaan G. Verhulst, Comparative Analysis of International Co- and Self- regulation in Communication Markets, Research report (commissioned by OFCOM), 2007, at:
http://www.mediachange.ch/media/pdf/publications/latzer_et_al_2007_comparative_analysis.pdf

[11] Mifsud Bonnici, J.P., Self-regulation in Cyberspace, T.M.C. Asser Press: The Hague, 2008 p.23

notare due diverse tendenze: mentre il codice FEDMA e la ICT coalition sono nati per iniziativa dei privati, la CEO coalition ed i SNS principles sono il risultato di una forte pressione della Commissione Europea. Di conseguenza, i questi ultimi due casi, manca la motivazione dei privati per affrontare i rischi della privacy online per i bambini, creando un importante fattore di diminuzione del supporto e di conseguenza la riduzione di tutto il processo di self-regulation.

Il secondo indicatore dei criteri di adozione si riferisce all'uso effettivo delle norme di self-regulation tra gli attori privati. Iniziative più efficaci sono considerate quelle in cui i partecipanti rappresentano il maggior numero possibile di potenziali attori del settore in questione. Gli SNS principles, a prima vista, appaiono come uno strumento altamente approvato dai soggetti ai quali si rivolge, raccogliendo 21 social networks providers, che rappresentano quelli più diffusi tra i giovani europei. Malgrado questo, ad un livello più ampio, i 21 social networks providers partecipanti costituiscono solo un quarto della fornitura di servizi social in Europa.

Solo nel 2009-2010, l'EU Kids Online Survey ha identificato circa 80 principali social networks utilizzati nel territorio europeo. Tenuto conto di tale stima, i SNS principles vengono scarsamente utilizzati dai titolari di social network, anche se la privacy dei loro utenti, potrebbe avere un forte impatto sulla scelta da parte dell'utente di iscriversi al servizio.

Il livello di adesione è altrettanto basso nel ICT e CEO coalition, che raccolgono rispettivamente 25 e 31 aziende del settore. Anche se le coalition comprendono varie industrie e vari settori, che vanno da quelle dei cellulari, delle telecomunicazioni, social gaming, produzione di contenuti, e tenuto conto dell'elevato numero di fornitori di servizi online, il livello di rappresentazione adeguata del settore è discutibile.

In contrasto con i tre precedenti, il codice FEDMA sembra essere adottato da un organismo rappresentativo in termini di partecipazione ed appartenenza alla zona diretta di marketing online. È l'unica organizzazione in questo settore a livello dell'Unione Europea che descrive se stessa come una *"voce unica di marketing diretto e interattivo europeo*[12]*"*. L'appartenenza al FEDMA, anche se volontaria, richiede l'adozione dei suoi codici di autoregolamentazione. Il codice FEDMA rappresenta un'interessante caso di utilizzo dei membri del FEDMA. La FEDMA afferma che *"applica il codice indipendentemente da qualsiasi azienda che fa marketing diretto in Europa, anche se non si tratta di un membro di FEDMA o delle associazioni nazionali di direct marketing (DMA)."* Sembra che il suo campo di applicazione sia esteso al di là dei suoi membri e sia percepito come uno standard nel settore del marketing diretto europeo.

Infine è rilevante analizzare se i quattro strumenti godano di sostegno pubblico in termini di obiettivi e metodi di regolazione. Il sostegno pubblico per gli obiettivi dei quattro strumenti sopra descritti è senza dubbio elevato. Le generali preoccupazioni sui problemi di sicurezza per i bambini e la privacy online sono ben documentati da diversi rapporti e sondaggi d'opinione. Ad esempio, quasi tutti gli europei (95%) sono convinti che i minori

[12] http://www.fedma.org/index.php?id=34

necessitano di protezione per quanto riguarda la loro privacy e la raccolta di dati online[13]. Tuttavia esistono opinioni diverse sul metodo e modo di come tale protezione specifica dovrebbe essere garantito. Alcune iniziative, come quelle CEO coalition e SNS principles, hanno incontrato il muro della società civile e delle organizzazioni per i diritti civili a causa della loro limitata capacità di affrontare efficacemente il problema per cui sono stati realizzati. La European Digital Rights (EDRi), associazione no-profit sui diritti civili digitali, ha affermato che gli SNS principles *"hanno fatto poco più che riassumere la normativa esistente, vestendola di un approccio di autoregolamentazione"*[14], mentre la CEO coalition è stata criticata per non aver messo a fuoco il tema che si era prefissate per la debolezza degli elaborati.
Riassumendo, il codice FEDMA ha ottenuto un punteggio più alto, in quanto il numero di partecipanti al codice è più alto ed ampiamente utilizzato nel settore della commercializzazione diretta ed online. Oltre alla sua applicabilità ai membri FEDMA, il codice si applica teoricamente a qualsiasi società che faccia marketing diretto e può essere invocata dalle autorità nazionali per la protezione dei dati. Tuttavia tale strumento non ha subito un elevato coinvolgimento dalle istituzioni pubbliche. I restanti tre strumenti sono, invece, poco rappresentativi dei rispettivi settori.

4.2 L'azione degli strumenti di self-regulation

Il criterio dell'azione si concentra sulla produzione di regolamentazione piuttosto che sul processo di regolamentazione, come nel caso dell'adozione. In particolare gli strumenti di self-regulation sono valutati in termini di rispetto ed applicazione degli schemi. Altri parametri sono il numero di reclami ricevuti, le controversie trattate, le possibili sanzioni per il mancato rispetto e la presenza (o assenza) di minacce da parte delle autorità pubbliche di intervenire.

4.2.1 Monitoraggio

Al fine di misurare il rispetto degli strumenti di self-rgulation, si monitorano le diverse attività di ciascuna iniziativa. Il rispetto dei SNS principles, viene periodicamente misurata attraverso valutazioni effettuate da esperti esterni. La valutazione è stata effettuate considerando due fasi: valutazione delle singole autodichiarazioni dei SNS providers e le prove pratiche dei loro siti web. Secondo la valutazione effettuata nel 2011, solo 3 delle 14 autodichiarazioni sono state valutate come "molto soddisfacenti", mentre 9 sono state dichiarate come "piuttosto soddisfacenti" e 2 come "insoddisfacenti"[15]. Le auto-valutazioni

[13] Special Eurobarometer 359, Attitudes on Data Protection and Electronic Identity in the European Union, June 2011, in http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

[14] European Digital Rights, 2013, *CEO Coalition – the blind leading the bland*, at: http://edri.org/ceo_coalition

[15] Assessment of the Implementation of the Safer Social Networking Principles for the EU on 14 websites: Summary Report, 2011, in http://www.unav.edu/matrimonioyfamilia/b/top/2011/UE_Donoso_Safer-so-

sono state meglio valutate in base alla loro reale implementazione sui siti web ed ai problemi che gli utenti avrebbero potuto avere durante la navigazione. Per quanto riguarda la privacy, gli SNS provider hanno dimostrato la loro maggiore carenza, in quanto solo 3 su 14 sono stati dichiarati come "molto soddisfacenti". La principale debolezza dei sistemi, si è verificata in relazione alla mancanza di informazione esplicita in merito alle caratteristiche di impostazioni della privacy e la mancanza di informazioni in merito ai supporti utili per una corretta configurazione della privacy.Anche se la maggioranza degli SNS providers ha dimostrato dei progressi positivi, il settore della privacy continua a mantenere delle carenze.
Analogamente agli SNS principles, la ICT coalition ha recentemente introdotto un monitoraggio indipendente per valutare come i membri della coalizione attuano i principi in materia di ICT. Diversamente dagli SNS principles, i membri della ICT coalition sono stati valutati sulla base delle loro dichiarazioni, senza prove effettive sui loro prodotti e servizi. Tale sistema di valutazione, però, non può essere esente da critiche. Data la tendenza dei membri a dichiarare più di quanto effettivamente attuato, solo una valutazione formale dei risultati potrebbe avere un impatto sulla valutazione obiettiva dei risultati. Il rapporto, sembra più una sintesi di buoni risultati, piuttosto che una valutazione obiettiva.
Il CEO coalition non subisce alcun sistema di monitoraggio formale. Il monitoraggio è stato effettuato durante il primo anno di funzionamento del CEO, ma era stato molto vago. Nel complesso si era riconosciuto che il progresso era stato effettuato in tutte e cinque le aree di lavoro. Nel Febbraio 2013, l'amministratore delegato della CEO coalition ha pubblicato la sua relazione finale contenente raccomandazioni e migliorie da poter adottare, mentre nel gennaio 2014, le imprese individuali hanno prodotto relazioni distinte su come hanno adottato ed adotteranno le raccomandazioni della coalizione.
La situazione, almeno sulla carta, è differente per il codice FEDMA che adotta un meccanismo di monitoraggi specifico. L'onere del monitoraggio è affidato ad un "Comitato per la protezione dei dati" che è stato istituito per monitorare l'applicazione del codice.

4.2.2 Reclami e Controversie

Teoricamente l'applicazione dipende dall'esistenza e dalla possibilità di accedere alle procedure per gestire possibili reclami in relazione alle norme di self-regulation e le conseguenze per i membri in caso di violazione. L'unico strumento self-regulation che prevede una procedura di ricorso è il codice FEDMA. Tale codice, essendo uno strumento europeo, dedica una parte alla definizione delle procedure per risolvere eventuali reclami che possono derivare dall'applicazione del codice stesso. Il reclamo viene analizzato dal "Comitato per la protezione dei dati", organo interno, composto da rappresentanti di associazioni nazionali di marketing diretto, il FEDMA e le aziende che sono membri diretti del FEDMA.

cial-networking-part1.pdf

4.2.3 Sanzioni

Altra carenza che si verifica nella maggior parte degli strumenti di self-regulation, è la mancata esecuzione delle sanzioni quando le violazioni delle norme di autoregolamentazione si verificano.Tale carenza si verifica per l'assenza di organismi specifici in grado di far rispettare tale sanzione.
Un riferimento esplicito alle sanzioni è presente solo nel codice FEDMA. Ai sensi del codice, le associazioni nazionali di direct marketing sono responsabili per l'applicazione del codice e devono applicare le stesse sanzioni previste nei loro paesi per il mancato rispetto dei loro codici nazionali.
Inoltre, a seconda del tipo di violazione, il Comitato per la protezione dei dati può raccomandare al FEDMA di espellere un membro o applicare sanzioni.[16]
Nella pratica non è chiaro quante volte la FEDMA abbia applicato come sanzione l'espulsione. Inoltre FEDMA non è in grado di imporre multe o applicare sanzioni monetarie, poiché è un'organizzazione di adesione volontaria.
In misura minore, ma simile, una possibilità sanzionatoria è presente nell'ICT Coalition. Si afferma che "se un membro non intende applicare i principi, può essere sottoposto ad esclusione".Tuttavia, non è ancora possibile sapere in che misura la ICT coalition abbia applicato tale principio.Altre due iniziative vengono utilizzate come meccanismi sanzionatori simbolici, connessi alla "reputazione delle imprese". Nel caso di scarso rendimento o non conformità ai SNS Principles, la Commissione Europea non ha mezzi formali per migliorare il rendimento, ma può pubblicare "rimproveri" verso le aziende che non riescono a rispettare tali principi.Tale sanzione simbolica può essere applicata nel caso del CEO coalition.

4.2.4 L'intervento del diritto sugli strumenti self-regulation

L'intervento del diritto da parte delle autorità pubbliche è considerato come un ulteriore incentivo ad adottare e rispettare le norme self-regulation. Oltre all'intervento esplicito, l'importanza e l'interpretazione del diritto vigente nell' Unione Europea, non dovrebbe essere scartato.
Anche se le istituzioni comunitarie non hanno mai minacciato pubblicamente le imprese con precise disposizioni di legge qualora gli strumenti self-regulation non fornissero i risultati attesi, alcuni segni indicano che la Commissione Europea si stia muovendo in tale direzione. Nel contesto della revisione del quadro di protezione dei dati personali, una possibilità di affrontare la protezione della privacy del minore è stata considerata. La consultazione pubblica, ha rivelato la volontà delle aziende di sviluppare dei codici di condotta in combinato disposto con l'art. 29 Working Party, per garantire la concreta applicazione.Appare discutibile, però, che l'intervento della Commissione Europea attraverso la protezione dei dati, abbia avuto influenza su una migliore osservanza dei regimi di self-regulation. Un punteggio basso sulla conformità al diritto, può esser assegnato alla

[16] Codice FEDMA p.18

CEO coalition, dove si valuta il loro lavoro, senza una supervisione o controllo esterno. In questo modo non è possibile stabilire quanto le singole imprese seguano i consigli e le migliori pratiche previste dalla coalizione.
Un livello di conformità più chiaro, seppure basso, è dato nel SNS Principles, dove vengono effettuate valutazioni indipendenti. Tuttavia in caso di scarsa aderenza, non vi è possibilità di applicare sanzioni efficaci e commercialmente significative.
La ICT coalition, ha una indipendente procedura di monitoraggio e prevede la possibilità di escludere aziende che che violino i principi in materia di ICT. Il codice FEDMA ha tutti gli aspetti necessari a garantire e misurare la conformità: una struttura organizzativa, una procedura di reclamo e potere sanzionatorio. Tuttavia, questo non garantisce le periodiche revisioni e valutazioni. Pertanto anche se promettente sulla carta, il codice FEDMA nella pratica non assume tale efficacia.

5. Riflessioni Conclusive

Il raggiungimento del self-regulation in un settore delicato come quello della privacy del minore, non è facile malgrado siano stati realizzati quattro strumenti per raggiungere tale finalità. Sulla base dell'analisi effettuata utilizzando il sistema di Latzer, si è visto come i quattro strumenti, il safer social networking, il CEO coalition, l'ICT coalition ed il FEDMA non abbiano ottenuto i risultati sperati.
Una possibile risposta alle attuali carenze, potrebbe rinvenirsi nell'intervento da parte della Commissione Europea ad un approccio di co-regolamentazione più forte e meglio definito sul fronte della sicurezza online del minore.
Tale soluzione potrebbe essere attuata, in quanto l'area della privacy dei bambini su Internet difficilmente può essere immaginata come solo strumento di self-regulation. Realizzare degli strumenti self-regulation che, magari, hanno una buona struttura normativa, ma non sorretti da una forte e decisa politica di sanzioni sottoposta ad un controllo da parte dell'Unione Europea, porta facilmente gli operatori del diritto a non rispettare tali strumenti. Solo un buon strumento di co-regolamentazione è in grado di realizzare innovazione, consentire un apprendimento reciproco, sensibilizzazione, condivisione di risorse tra gli operatori e le altre parti interessate.
Ciò risulta in linea con il ragionamento della Commissione Europea, dietro la creazione di piattaforme multi-stakeholder normative. Come spiegato da Neelie Kroes *"Abbiamo bisogno di incoraggiare l'innovazione, scambiare idee e condividere le risorse. E abbiamo bisogno di continuare a costruire un'infrastruttura trans-europea per tutelare e proteggere i bambini(…)"*[17].

[17] Neelie Kroes Vice-President of the European Commission responsible for the Digital Agenda Making Internet a better place for children – a shared responsibility Safer Internet Forum 20 October 2011, Luxembourg, Reference: SPEECH/11/703, 20/10/2011, at http://europa.eu/rapid/press-release_SPEECH-11-703_en.htm

N. 3 - 2015 · pp. 51-78

Open (big) data, tra implicazioni di potere e prospettive di evoluzione cognitiva della specie

Giovanni Crea

Abstract: Il fenomeno *big data* è una delle espressioni di quell'ecosistema digitale, chiamato internet, in cui le attività degli organismi viventi che vi fanno parte (gli individui) si caratterizzano per l'uso sistematico delle tecnologie dell'informazione e della comunicazione (Ict). La formazione di grandi e complesse masse di dati ha origine proprio dal costante impiego delle Ict (e di internet che ne è il 'prodotto' più rappresentativo). L'evoluzione in tal senso della società (società dell'informazione, *network society*) ha messo in evidenza il collegamento dei *big data* con altri capitoli legati alle predette tecnologie: l'apertura e il riutilizzo dei dati – o, per meglio dire, dei contenuti – detenuti dalle pubbliche amministrazioni, la privacy, ma anche il potere di taluni *over the top* che operano nella grande Rete. Le questioni che ne derivano sono riconducibili a un conflitto tra gli interessi delle figure coinvolte che il diritto è chiamato a fronteggiare con gli stessi strumenti tecnologici, assumendo pertanto una connotazione *compliance* all'ecosistema digitale che può essere definita *law and technologies*.

The *big data* phenomenon is one of the expressions of that digital ecosystem, called internet, in which the activities of living organisms that are part of (individuals) are characterized by the systematic use of information and communication technologies (Ict) .The formation of large and complex data sets has originated from the constant use of Ict (and internet, who is the 'product' more representative). The evolution in this direction of the society (information society, network society) has highlighted the connection of big data with other issues related to the above technologies: the opening and re-use of data – rather, the content – controlled by governments, privacy, but also the power of certain *over the top* in internet. The resulting problems are due to a conflict between the interests of actors involved that law must deal with the same technological tools, assuming a connotation compliance digital ecosystem that can be defined law and technologies.

Parole chiave: big data, riutilizzo dei contenuti, Ict, ecosistema digitale, potere di mercato, lavoro cognitivo, capitalismo cognitivo.

Articolo pervenuto il 10 febbraio 2015, approvato il 20 febbraio 2015

1. Introduzione.

L'esperienza della società *post*-industriale, teorizzata da Daniel Bell nel 1973[1], ha messo in luce vantaggi e rischi di un modello socioeconomico in cui i rapporti tra i suoi membri sono mediati dalla grande Rete. Le politiche internazionali sono univocamente determinate nella transizione verso questo modello, e ciò perché le prospettive di benessere sociale e le implicazioni di libertà possono davvero cambiare in meglio le condizioni e le attività umane, a patto, però, che si risolvano sotto il profilo giuridico e dell'intervento regolamentare le criticità di segno contrario. A tal riguardo, va rilevato come gli ordinamenti statali si siano trovati a dover fare i conti con la spinosa questione riguardante il loro stesso aggiramento permesso dalla Rete, la cui soluzione non sembra essere proprio a portata di mano; con l'espansione e la «colonizzazione»[2] di internet, il diritto è apparso da sùbito più debole di fronte a comportamenti di violazione di una qualche regola incoraggiati soprattutto dalla possibilità (e dalla capacità) di mantenere l'anonimato; comportamenti che vanno dal *profiling* degli utilizzatori della Rete effettuato a loro insaputa all'immissione (e conseguente diffusione) in rete di contenuti coperti da diritti di proprietà. La regolazione internazionale coordinata e l'approccio *law and technologies* – vale a dire, l'impiego delle tecnologie dell'informazione e della comunicazione (Ict) nel ruolo di braccio operativo del diritto – hanno rappresentato alcune ipotesi che, tra scetticismo e ottimismo, sono ancora dibattute in dottrina e nelle sedi istituzionali. A queste si è aggiunta, sul versante europeo e con particolare riguardo alla protezione dei dati personali, la proposta di un'applicazione della disciplina anche ai casi in cui il trattamento dei dati avviene in un territorio extraeuropeo, facendo perno sul requisito della residenza degli interessati nell'Unione europea, onde evitare che tali individui possano essere privati della tutela apprestata dal diritto comunitario[3]. La prospettiva dell'adozione di una norma di tal fatta – che non ha mancato di suscitare qualche perplessità sulla sua effettiva applicazione – costituisce una forma di pressione sui fornitori di servizi che si avvalgono di infrastrutture allocate oltre i confini dell'Unione, essendo destinata a incidere sugli accordi che regolano i rapporti tra gli stessi *provider* e gli utenti. Al riguardo, va ricordato come la questione della *applicable law* costituisca il principale aspetto critico del fenomeno *cloud computing* alla luce delle esigenze di sicurezza manifestate dal lato della domanda delle imprese.

Quello dei *big data* – termine con cui la letteratura e gli analisti descrivono la formazione di insiemi complessi di contenuti – è un capitolo entrato recentemente a far parte del quadro degli argomenti che descrivono, sotto aspetti diversi, la società *post*-industriale e

---

1 Cfr. D. Bell, *The Coming of Post-Industrial Society. A Venture in Social Forecasting*, New York, 1973.

2 Il termine è di G. Sartor, *Il diritto della rete globale*, in *Ciberspazio e diritto*, vol. IV, n. 1, 2003, 67-94.

3 Al riguardo, cfr. Commissione europea, *Proposta di Regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati*, 25 gennaio 2012, considerando n. (20) e art. 3. In tali casi, l'applicazione extraterritoriale della disciplina riguarda i trattamenti connessi all'offerta di beni o servizi agli interessati residenti nell'UE o al monitoraggio del loro comportamento.

le sue evoluzioni. La complessità di questi insiemi va ricondotta non tanto (e, comunque, non solo) al profilo dimensionale, ma anche alla varietà dei contenuti, al loro carattere non strutturato, alla diversità dei formati[4]. Anche questo fenomeno – al pari di altri che caratterizzano l'ecosistema digitale – mostra quel duplice profilo che pone a confronto gli effetti di segno opposto che esso è suscettibile di determinare, e per il quale – come spesso accade – è opportuno adottare una qualche misura regolamentare che possa tener conto dell'equilibrio tra gli interessi in gioco. Guardando al lato virtuoso dei *big data*, va preliminarmente osservato che le prospettive di crescita dei contenuti digitali (dati, informazioni, conoscenze), delineate dall'impiego sempre più costante delle ICT, non fanno che suggellare il primato di queste risorse nelle scelte pubbliche e private. Sotto il profilo dimensionale, merita segnalare come il volume di contenuti circolante nell'ambiente digitale – stando alle stime fornite dalla IDC (International Data Corporation) in una sua ricerca del 2012[5] – si sia attestato intorno ai 2,8 ZB (l'unità di misura ZB equivale a 10^{21} byte), con previsioni di crescita che si collocano su livelli di 40 ZB entro il 2020. Va da sé che la gestione di simili masse di contenuti riposa sull'impiego di tecnologie e metodi di analisi specifici la cui capacità può portare alla luce fenomeni (o taluni loro aspetti), altrimenti ignorati, suscettibili di essere indagati sul piano statistico; e, anzi, sotto questo profilo, l'enfasi pare appuntarsi sui possibili sviluppi di una disciplina specifica dei *big data* (*big data computing*) che si distingue dalle tradizionali analisi dei dati richiedendo risorse e competenze capaci di estrarre dalle grandi aggregazioni di contenuti il valore massimo in termini di conoscenza[6]. Al riguardo, la stessa IDC nel suo studio avverte dell'esistenza di un divario tra il valore potenziale racchiuso nei grandi *data set* e quello effettivamente ricavato dagli stessi (*big data gap*). Gli esiti di conoscenza che derivano dal trattamento dei *big data* sono quanto meno intuibili: il servizio sanitario, l'ambiente, l'economia, rappresentano alcuni dei settori di interesse in cui l'analisi di grandi insiemi di contenuti determina una maggiore cognizione dei fenomeni e dei processi che, a sua volta, può supportare le decisioni di operatori pubblici e privati. Al riguardo, basti pensare alla possibilità di applicare la *big data computing* a dati ambientali e dati sanitari da cui poter ricavare un *output* cognitivo utilizzabile in chiave preventiva, ad esempio per

---

[4] I contenuti non strutturati (o dati non strutturati) si distinguono per il fatto di non essere organizzati in un *data base* secondo un determinato schema di classificazione. I contenuti non strutturati sono in massima parte riconducibili all'avvento di internet; in tale contesto si generano notevoli quantità di contenuti attraverso le diverse forme di comunicazione (*e-mail*, sms, tweet) e di espressione (pubblicazioni di fotografie e contenuti audiovisivi sui *social media*) che, evidentemente, non seguono schemi predeterminati. Il formato di un contenuto denota la modalità con cui esso è stato codificato (ossia convertito in una successione di bit).

[5] Cfr. IDC, *The Digital Universe in 2020: Big Data, Bigger Digital Shadows, and Biggest Growth in the Far East*, december 2012.

[6] La gestione dei *big data* richiede strumenti diversi da quelli tradizionali che si caratterizzano per la loro velocità di trattamento, vale a dire per la capacità di analizzare i dati in tempi brevi. Nella prospettiva di molti analisti, il fattore della velocità (che riguarda direttamente il *software*) unitamente alla dimensione e alla varietà (che, invece, si riferiscono ai dati), individuano i *big data*. Al riguardo si veda DEDAGROUP, ECOS, *Big data: riconoscerli, gestirli, analizzarli*, documento reperibile all'indirizzo <http://www.ecos2k.it/allegati/BigData.pdf>; P. PASINI, A. PEREGO, *Big data: nuove fonti di conoscenza aziendale e nuovi modelli di management*, ed. SDA Bocconi School of management, 2012.

indirizzare talune politiche locali.
Il fenomeno dei *big data* ha però il suo rovescio della medaglia, rappresentato dal rischio che i detentori di grandi masse di contenuti, possano derivarne un potere, in particolare sotto il profilo della capacità elaborativa[7], di cui non vanno sottovalutate le possibili ricadute sociali. Scenario, questo, piuttosto inquietante se si considera che il vantaggio ascrivibile alla capacità di trattamento dei *big data* riposa sul possesso di adeguate risorse *hardware* e *software* che, verosimilmente, non sono alla portata di tutti; sotto quest'ultimo aspetto, merita sottolineare come, chi non dispone di una capacità informatica calibrata sulla complessità di tali insiemi possa, al più, estrarre un *output* limitato[8], se non perfino incorrere nelle controindicazioni dell'eccesso di informazioni da più parti messe in evidenza[9]. Il profilo dei detentori dei *big data* è riconducibile a operatori pubblici e privati che raccolgono una notevole quantità di contenuti nell'ambito delle loro attività istituzionali ed economiche. La loro fisionomia è facilmente intuibile, per non dire scontata, trattandosi di pubbliche amministrazioni da un lato e, dall'altro, di imprese di notevoli dimensioni – come Walmart, il colosso americano della grande distribuzione – di fornitori di servizi di interesse economico generale – spesso *ex* monopolisti – e, ancora, di imprese che forniscono servizi internet etichettate come *over the top*; il potere che può derivare dal controllo dei *big data* si qualifica essenzialmente sotto due profili: la detenzione di una posizione dominante nei mercati in cui essi operano e il controllo sociale. Sul piano del mercato, la concentrazione dei *big data* delinea la costituzione di posizioni di potere le cui rendite economiche rischiano di marginalizzare gli effetti di benessere sociale rispetto a una situazione di redistribuzione dei contenuti informativi e conoscitivi. A ciò va aggiunta la prospettiva di comportamenti dei detentori che possono limitare le libertà fondamentali e, nel caso del settore pubblico, possono ostacolare i processi di *open government* che, nel nome della trasparenza, implicano l'introduzione di meccanismi atti a favorire forme di controllo da parte della società civile.
Le politiche di apertura e di riutilizzo dei *big data* delle pubbliche amministrazioni rappresentano una risposta al fenomeno della concentrazione appena tratteggiato. Sotto il profilo cognitivo, siffatte iniziative sono volte a favorire la disseminazione dei contenuti e, con essa, l'evoluzione intellettuale, nella prospettiva di riequilibrare le asimmetrie di posizione che da sempre connotano i rapporti tra imprese dominanti e *new entrant*, tra imprese e consumatori, e, ancora, tra settore pubblico e società civile. Gli effetti attesi di questo riequilibrio vanno dunque ricondotti a situazioni di maggiore concorrenza, di

---

[7] Al riguardo, si veda A. Mantelero, *Big data*: *i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo*, in *Dir. Inf. Inf.*, n. 1, 2012; C. Flick, V. Ambriola, *Dati nelle nuvole: aspetti giuridici del cloud computing e applicazione alle amministrazioni pubbliche*, in *federalismi.it*, n. 6, 2013.

[8] Sul punto si veda A. Mantelero, *Big data*: *i rischi della concentrazione del potere informativo digitale*, *op. cit.*

[9] Cfr. D. Schenk, *Data smog: surviving the information glut"*, New York, HarperCollins, 1997. L'autore sottolinea come un eccesso di informazione (descritto con la metafora *smog*) possa avere implicazioni negative sotto il profilo gestionale; superato un certo livello, il carico informativo non ha più effetti virtuosi. Sul tema, con particolare riferimento ai *social network*, si veda anche G. Riva, *I social network*, Bologna, Il Mulino, 2010.

empowerment dei consumatori, di controllo da parte della società civile dell'operato delle pubbliche amministrazioni. Al riguardo, va osservato come la prima stagione legislativa, inaugurata dalla direttiva 2003/98/CE e protrattasi per un decennio, abbia prodotto risultati esigui sul fronte dell'accesso e del riutilizzo dei contenuti, principalmente in ragione dell'assenza di un obbligo per il settore pubblico di operare in tal senso; condizione, quest'ultima, a cui il legislatore ha posto rimedio (sia pure dopo due lustri) con il passaggio a un regime prescrittivo sul riutilizzo avvenuto con la direttiva 2013/37/UE. Un tale adeguamento segna una fase fondamentale dell'agenda digitale europea, implicando la rimozione di un ostacolo giuridico-culturale che per lungo tempo è prevalso sull'interesse alla circolazione e alla valorizzazione dei contenuti. La previsione dell'uscita dei contenuti dal perimetro pubblico non può che imprimere maggiore impulso al lavoro cognitivo – la creatività, l'innovazione e altre abilità soggettive – fattore produttivo centrale di un'economia il cui motore di crescita è individuato nella conoscenza.

2. Politiche di apertura dei contenuti.

L'accesso ai contenuti è una condizione essenziale per lo sviluppo socio-economico di un paese in ragione del «valore» che l'impiego di queste risorse è suscettibile di generare. La conoscenza è già essa stessa un valore; è il risultato del trattamento di informazioni e altre conoscenze ed è esplicativa delle decisioni degli agenti pubblici e privati: politiche economiche e sociali, strategie d'impresa, produzione di nuova conoscenza (idee innovative, opere dell'ingegno, nuove teorie). Il ruolo di questa risorsa era ben chiaro anche alla teoria economica neoclassica laddove nel formulare i modelli della concorrenza perfetta e della concorrenza monopolistica ipotizzò, tra l'altro, uno stato informativo ottimale delle imprese, come se la circolazione dei contenuti fosse scontata; ipotesi che lascerebbe quasi intendere che l'ideale *open data* non è una novità della recente politica economica occidentale, salvo poi verificare come nel tempo una tale ipotesi non sia stata pienamente realizzata. Sotto quest'ultimo aspetto, l'esperienza dei grandi *trust* – le grandi imprese industriali di John D. Rockefeller, Henry Ford e di pochi altri – racconta di un utilizzo in forma chiusa della conoscenza tecnico-scientifica, fatta da un lato (gli operai) di specializzazioni e *routine* organizzative applicate con l'intento di aumentare la produzione e conseguire le economie di scala, e dall'altro (la classe dirigente) di sapere manageriale utilizzato per guidare i consumi nella direzione voluta dai produttori; esempio emblematico di un'asimmetria conoscitiva che per lungo tempo ha favorito il potere di mercato sia come limitazione della concorrenza sia come egemonia della produzione sul consumo. Non va peraltro sottaciuto come per effetto del progresso tecnologico e sociale che ha caratterizzato il periodo successivo alle grandi concentrazioni di mercato (*post-fordismo*), la conoscenza sia divenuta una risorsa «visibile» e, soprattutto, non più esclusiva dei gruppi dominanti; la conoscenza ha iniziato a decentrarsi – anche grazie alla mediazione delle reti – e l'impresa *post-fordista* ne ha intrapreso l'utilizzo, acquisendola dai mercati del lavoro cognitivo, dalle licenze di sfruttamento di contenuti e opere nate

dall'ingegno dell'uomo, dall'accesso al codice sorgente del *softaware*[10].
Il tema della conoscenza ha una radice in quelle iniziative internazionali volte a promuovere l'accesso alle risorse digitali a scopo di riutilizzo, risorse le cui prospettive di sfruttamento hanno attirato in poco tempo l'attenzione di studiosi ed esperti di diversa provenienza disciplinare per le implicazioni di utilità per l'economia e per la società. In questo scenario hanno preso corpo le politiche *open data*, poste in essere con intenti di valorizzazione dei *big data* del settore pubblico, da cui l'Europa come gli USA si aspettano ricadute positive sulle rispettive economie. Politiche che, invero, partono da lontano (in Europa, nel luglio del 1989, con la pubblicazione, da parte della Commissione europea, delle *Linee direttrici per migliorare la sinergia dei settori pubblico e privato nel settore dell'informazione*; negli *States*, con il più risalente *Freedom of Information Act* promulgato nel 1966), e alle quali si è affiancato quell'attivismo che negli ultimi venti anni ha sostenuto l'accesso all'informazione e alla conoscenza come realizzazione di un principio di libertà. Dopo le campagne di Richard Stallman e Linus Torvalds a favore del *software* libero (*open source*) e dopo l'estensione di tali iniziative alla categoria dei contenuti grazie al contributo di Lawrence Lessig, le istanze dei movimenti e della società civile in genere si sono rivolte anche all'"informazione del settore pubblico". In quest'ultimo caso, è la dottrina dell'*open government data* a rivendicare, in seno al principio della trasparenza, la disponibilità di queste risorse in possesso degli enti pubblici principalmente per esigenze di controllo dei processi di governo[11] (ma non escludendo un loro riutilizzo nell'ambito dell'iniziativa economica). Gli effetti positivi dell'uso diffuso di risorse immateriali, rappresentative di informazioni e conoscenze codificate, sono ormai di comune dominio, e ciò spiega come il movimento *open data* abbia finito per intrecciarsi con le *policies* comunitarie e d'oltreoceano; al riguardo, vanno richiamate la direttiva europea del 2003 sul riutilizzo dell'informazione del settore pubblico (Psi *directive*) e l'*Open government directive* adottata nel dicembre 2009 dall'amministrazione Obama, alle quali va riconosciuta la volontà di superare le logiche conservative e proprietarie del settore pubblico[12] che, per lungo tempo, ne hanno fornito l'immagine di un'autorità collocata su un piano decisamente distante dalla società civile[13]. L'intento di queste iniziative regolamentari, dunque, è stato quello di incoraggiare un mutamento culturale del settore pubblico che, in tale prospettiva, è chiamato a favorire attività economiche a valore aggiunto connesse al trattamento di risorse informative pubbliche. Le stime sulla determinazione di un valore incrementale fornite dai rapporti europei e statunitensi lasciano ben sperare sulla riuscita di una riforma

---

[10] Cfr. E. Rullani, *La conoscenza e le reti: gli orizzonti competitivi del caso italiano e una riflessione metodologica sull'economia di impresa*, in *Sinergie*, vol. 21, n. 61-62, 2003, 147-187.

[11] Cfr. F. Di Donato, *Lo stato trasparente*, Pisa, ETS, 2010; T. Agnoloni, M.T. Sagri, D. Tiscornia, *Open data: nuova frontiera della libertà informatica ?*, in *Informatica e diritto*, n. 2, 2009, 7-19.

[12] In tal senso, F. Merloni, *Coordinamento e governo dei dati nel pluralismo amministrativo*, in B. Ponti (a cura di), *Il regime dei dati pubblici*, Rimini, Maggioli, 2008.

[13] Sul punto, sia consentito un rinvio a G. Crea, *Il settore pubblico e la tutela degli utenti nella prospettiva della cloud economy*, in *Diritto, economia e tecnologie della privacy*, n. 2, 2012, 235-268, in particolare 248, 249.

che comproverebbe il potenziale economico dell'apertura alle *public sector information* (Psi); una ricerca pubblicata dalla McKinsey nel 2011, ad esempio, ha concluso che il riutilizzo (efficace) dei dati potrebbe determinare un valore aggiunto valutato attorno ai 300 milioni di dollari su base annua[14]. La società *post*-industriale, dunque, non può che essere *open* sia pure all'interno di un equilibrio in cui vanno salvaguardati altri interessi; il che, sotto il profilo del diritto, implica che, in talune situazioni, in cui si pongono questioni di sicurezza nazionale, *data protection*, tutela della proprietà intellettuale, l'*open society* deve mettere in conto l'adozione di forme di limitazione dell'accesso ai contenuti e del loro reimpiego, ricorrendo, in alcuni casi, a meccanismi che garantiscono l'autodeterminazione informativa, in altri a regìmi di licenze e, in altri ancora, all'esclusione dell'accesso. Va da sé che, seguendo il principio della proporzionalità, la dimensione delle predette restrizioni dovrebbe essere quella minima necessaria agli scopi di tutela, per non ostacolare in modo ingiustificato l'altro obiettivo della riutilizzabilità. Sotto quest'ultimo aspetto, va rilevato che le licenze tradizionalmente «chiuse» non sempre appaiono proporzionate agli scopi; in un siffatto regìme, la gamma dei diritti resta limitata alla semplice consultazione ed esclude trattamenti finalizzati alla creazione di contenuti derivati[15]. Con riguardo alla questione che vede la contrapposizione tra licenze *closed* e licenze *open*, va sottolineato come la dottrina abbia criticato la disciplina giuridica europea di protezione delle banche dati, introdotta dalla direttiva n. 9 del 1996, sottolineandone gli effetti di impedimento al reimpiego dei contenuti degli enti pubblici[16]; tra il diritto d'autore e il diritto (*sui generis*) giustificato dagli investimenti sostenuti per la costituzione di un *data base*, lo sfruttamento esclusivo e l'obiettivo del conseguimento di un margine economico hanno prevalso sull'interesse al riutilizzo generale dei contenuti[17]. A ciò deve aggiungersi che la citata direttiva del 2003, pur incoraggiando (ma non obbligando) gli enti pubblici a rendere disponibili le informazioni del settore per il loro riutilizzo (per finalità diverse da quelle originarie per le quali l'amministrazione li ha raccolti o prodotti), anche attraverso l'adozione di opportune licenze e con tariffe più abbordabili, non sembra aver inciso sull'equilibrio preesistente se non in modo frammentato[18]; un esito che la Commissione europea, nel riesaminare la Psi *directive*, ha imputato all'assenza, dal lato degli enti pubblici, di una visione più ampia che permettesse di cogliere i vantaggi per l'economia di un paese, e che ha favorito il persistere di ostacoli legati a interessi di recupero dei costi e di finanziamento delle attività

---

[14] Cfr. McKinsey Global Institute, *Big data: the next frontier for innovation, competition and productivity*, May 2011.

[15] In tal senso si veda A De Robbio, *OL4OD: licenze aperte per dati aperti*, in *JLIS.it*, vol. 2, n. 2, 2011.

[16] Cfr. direttiva 96/9/CE, *relativa alla tutela giuridica delle banche dati*, in *GUCE*, L 77, del 27 marzo 1996, p. 20 ss.

[17] Cfr. S. Aliprandi, *Open licensing e banche dati*, in *Informatica e diritto*, n. 1-2, 2011, 25-43; F. Di Donato, *Lo stato trasparente*, *op. cit.*

[18] In tal senso, sui contenuti della direttiva 2003/98/CE si vedano le annotazioni di I. D'Elia, *La diffusione e il riutilizzo dei dati pubblici. Quadro normativo comunitario e nazionale: problemi e prospettive*, in *Informatica e diritto*, n. 1, 2006, 7-46.

interne al settore pubblico[19], nonché a obiettivi di conservazione di una supremazia rispetto al settore privato. L'interoperabilità è l'altra questione rilevante che l'apertura dei dati, dal canto suo, ripropone; sappiamo, a tal riguardo, come la 'comunicabilità' tra sistemi derivati dalle Ict sia al centro delle politiche comunitarie volte a unificare mercati e servizi pubblici[20]. In questa prospettiva, la definizione di protocolli comuni (*standard*) per la comunicazione tra archivi pubblici indipendenti è – a dir poco – auspicabile per non limitare lo sfruttamento dei contenuti, rinunciando in tal caso all'utilità derivante dall'aggregazione di risorse di diversa provenienza. Sotto questo aspetto, l'opportunità di combinare contenuti di fonti diverse sta, oltre che nella possibilità di condurre analisi più puntuali sui fenomeni di interesse, anche e soprattutto nella prospettiva di scoprire profili fenomenici che, altrimenti, in assenza di interoperabilità, non emergerebbero; quest'ultimo aspetto può ben rappresentare una nuova frontiera per le scienze statistiche. Le condizioni di apertura ai contenuti pubblici e di interoperabilità tra sistemi informativi distribuiti si riassumono nel paradigma *linked open data*, la cui piena attuazione richiede interventi di *policy* su più fronti, tra i quali la regolamentazione tecnica, i programmi di finanziamento di progetti, la legislazione sul riutilizzo dei dati del settore pubblico. Questo paradigma apre a una prospettiva inedita, quella dell'accesso ad un archivio pubblico (equiparabile a un *big data*) formato secondo la logica *linked* e dunque avente una struttura di rete. A tal riguardo, rileva osservare come la tecnica del *collegamento* abbia dato vita al *web* tradizionale – il cosiddetto *web* dei documenti – il cui accostamento alla categoria *big data* è stato da più parti messo in evidenza[21]. Una siffatta architettura e le sue evoluzioni – il passaggio al *web* di dati, ad esempio[22] – possono rappresentare un valido rimedio ai possibili effetti oligopolistici legati al controllo dei *big data* da parte di pochi soggetti.

3. Verso l'*open* (*big*) *data*

L'apertura dei *big data* e l'utilizzo dei loro contenuti è un capitolo dell'Agenda digitale europea la cui realizzazione non è semplicemente una questione di norme e di tecnologie,

---

[19] Cfr. Commissione europea, *Riutilizzo dell'informazione del settore pubblico. Riesame della direttiva 2003/98/CE*, 7 maggio 2009, p. 3.

[20] Si veda, tra gli altri documenti, Commissione europea, *Verso l'interoperabilità dei servizi pubblici europei*, comunicazione del 16.12.2010; *Un'agenda digitale europea*, comunicazione del 26.8.2010; *Libro bianco. Ammodernamento della normalizzazione delle tecnologie dell'informazione e della comunicazione nell'UE – Prospettive*, comunicazione del 3.7.2009

[21] L'assimilazione del *web* ad un *big data* pubblico distribuito si coglie chiaramente nelle argomentazioni di G. Rizzo, F. Morando, J.C. de Martin, *Open data: la piattaforma di dati aperti per il linked data*, in *Informatica e diritto*, n. 1-2, 2011, 493-511. Gli autori affermano che il «Il tema dell'*Open Data* assume un'importanza strategica nel *Web* che diventa sempre più un enorme archivio pubblico distribuito di *Linked Data* […]».

[22] Cfr. T. Agnoloni, M.T. Sagri, D. Tiscornia, *Open data*, *op. cit.*, in cui gli autori, citando Tim Berners Lee, osservano che «l'evoluzione di Internet è rappresentata dal passaggio da una 'rete di documenti' verso una 'rete di dati'». Si veda anche Rizzo, F. Morando, J.C. de Martin, *Open data*, *op. cit.*; M. Guerrini, T. Possemato, *Linked data: a new alphabet for the semantic web*, in *JLIS.it*, vol. 4, n. 1, 2013.

ma richiede un vero e proprio cambiamento culturale. Sotto questo profilo, la prospettiva dell'*open data* dovrebbe essere quella di diventare una regola «sociale» più che giuridica, una prassi incardinata nella società della conoscenza; il che non escluderebbe la funzione del diritto che, in tale evenienza, dovrebbe comunque garantire che la libertà insita nella pratica *open data* non pregiudichi altre libertà e interessi, personali e generali (privacy, proprietà intellettuale, sicurezza), anch'essi meritevoli di tutela. Un simile passaggio segnerebbe un punto a favore della circolazione delle informazioni e delle conoscenze codificate[23], vale a dire di quel meccanismo che, con il supporto delle reti, dà luogo ad abilitazioni cognitive per individui e sistemi, alla moltiplicazione delle conoscenze e del valore. Sotto questo aspetto, il riutilizzo dei dati pubblici si inquadra nelle politiche comunitarie volte a promuovere quel modello socioeconomico che individua nella conoscenza[24] una nuova forma di capitalismo – il capitalismo cognitivo – destinato a subentrare a quello industriale con investimenti centrati sull'acquisizione di risorse cognitive[25]. Sappiamo peraltro che nella fase odierna di attuazione dell'agenda digitale, il paradigma dei dati aperti si scontra con gli interessi dei detentori di grandi banche dati, privati e pubblici, tradizionalmente guidati da logiche settoriali di potere e di controllo; l'*open data*, dunque, appare ancora lontano dal diventare un canone culturale, richiedendo evidentemente una qualche forma di regolazione.

Nel settore privato, in particolare nell'ambiente di mercato, dove le risorse conoscitive costituiscono una variabile competitiva, la prospettiva di una loro apertura appare decisamente meno realistica, e comunque non è una pratica generalizzata. In tale contesto, lo scambio di informazioni e conoscenze tra imprese è ipotizzabile se queste operano su mercati divergenti, laddove il loro sfruttamento da parte di un'impresa non ha implicazioni sulla rendita dell'altra[26]; ciò che avviene, ad esempio, nei sistemi industriali

---

[23] Il riferimento è a quella componente di conoscenza (esplicita) rappresentabile in forme strutturate e comprensibili. La conoscenza codificata è suscettibile di essere convertita in caratteri binari (digitali) e di essere trasportata attraverso una rete di telecomunicazioni. La letteratura distingue tra conoscenza esplicita e conoscenza implicita (tacita); quest'ultima è riconducibile all'esperienza lavorativa ed a capacità specifiche dell'individuo difficilmente codificabili e trasferibili. Sul concetto di conoscenza implicita si veda l'opera di M. Polanyi, *The Tacit Dimension*, New York, Anchor Books, 1966 (tr. it. *La conoscenza inespressa*, Roma, Armando ed., 1979). Sulla distinzione tra i due profili della conoscenza si veda anche I. Nonaka, H. Takeuchi, The knowledge creating company, Milano, Guerini e Associati, 1997.

[24] In tal senso si veda B. Ponti, *Titolarità e riutilizzo dei dati pubblici*, in B. Ponti (a cura di) *Il regime dei dati pubblici. Esperienza europee e ordinamento nazionale,* Rimini, Maggioli, 2008. L'autore sottolinea come la direttiva 98/2003/CE «[…] si inserisce in un più ampio contesto di politiche comunitarie volte ad incentivare le dinamiche economiche ma anche i processi culturali, sociali ed istituzionali della c.d. 'società della conoscenza' […]».

[25] Di qui, discende anche una nuova rappresentazione del lavoro che ne esalta il profilo cognitivo (lavoro cognitivo). Per questi argomenti si rinvia a E. Rullani, *Tecnologie che generano valore: divisione del lavoro cognitivo e rivoluzione digitale*, in *Economia e politica industriale*, n. 93, 1997, 141-168; E. Rullani, L. Romano (a cura di), *Il postfordismo: idee per il capitalismo prossimo venturo*, Milano, Etas, 1998.

[26] Sul punto si vedano le considerazioni svolte da S. Vicari, *Conoscenza e impresa*, in *Sinergie*, n. 76, 2008, 43-66, in particolare 48-49.

«distrettuali» attraverso la cooperazione e lo scambio di tecnologie[27].
Nel caso delle pubbliche amministrazioni, sono ben note le resistenze ai processi di apertura e di riutilizzo specie se si considera la finalità di conferire un potere di controllo alla società civile; resistenze che hanno trovato sostegno nelle norme sull'accesso ai documenti amministrativi, con il ricorso all'espediente del segreto amministrativo o al regime dell'accesso condizionato che subordina l'accoglimento delle istanze all'accertamento di un interesse particolare dei richiedenti (nel nostro ordinamento, un interesse corrispondente a una situazione giuridicamente tutelata e collegata al documento a cui si riferisce la richiesta di accesso)[28]. Sul punto, va osservato come la restrizione apportata da una disciplina dell'accesso non sia di per sé ingiustificata, potendosi ammettere che, per ragioni di tutela di situazioni giuridicamente rilevanti (al pari della privacy ovvero della proprietà intellettuale), taluni documenti amministrativi possano essere soggetti al più a un regime di conoscibilità limitata. Piuttosto, il lato critico va individuato in quei comportamenti delle amministrazioni tesi a sottrarre al riutilizzo «generalizzato» (libero) categorie documentali (o, comunque, parti di esse) per le quali, invero, l'esclusione dall'accesso o l'accertamento di un interesse particolare non appaiono giustificati. Sotto questo aspetto, le norme nazionali sull'accesso hanno beneficiato nel tempo di una piena autonomia[29] rispetto alle regole sul riutilizzo, ancorando l'accesso alla dimensione soggettiva e, per questo, costituendo un ostacolo per gli obiettivi del riutilizzo diffuso. Un

---

[27] La letteratura sul tema è vasta. Si veda, tra gli altri, A. Cresta, *Il ruolo della governance nei distretti industriali*, Milano, Franco Angeli, 2008, 18; A Tola, *Innovazione tecnologica, eco sostenibilità e sviluppo competitivo nel settore del sughero*, Milano, Franco Angeli, 2012, 47 ss.; I. Bonacci, *Lo sviluppo organizzativo nei distretti industriali. Il ruolo dell'ICT*, Milano, Franco Angeli, 2007, 119; L, Bottinelli, E. Pavione, *Distretti industriali e cluster tecnologici: strategie emergenti di valorizzazione della ricerca e dell'innovazione*. Milano, Giuffré, 2011, 16. Non va tuttavia escluso che gli accordi sullo scambio di informazioni possano realizzarsi anche tra imprese concorrenti; il che non implica che, in tali casi, la condivisione di informazioni sia *di per sé* restrittiva della concorrenza. Peraltro, le norme *antitrust*, in particolare l'articolo 101 del trattato sul funzionamento dell'Unione europea, avvertono del divieto di intese – nel caso in argomento, dello scambio di informazioni – ove queste possano pregiudicare il commercio tra stati membri e abbiano lo scopo o l'effetto di restringere la concorrenza. Sull'applicazione dell'articolo 101 del trattato, anche con riguardo allo scambio di informazioni, si veda Commissione europea, *Linee direttrici sull'applicabilità dell'articolo 101 del trattato sul funzionamento dell'Unione europea agli accordi di cooperazione orizzontale*, in *GUUE*, C 11, del 14 gennaio 2011, p. 16. La Commissione sottolinea (paragrafo 75) che «Nella valutazione degli effetti restrittivi sulla concorrenza si devono confrontare i probabili effetti dello scambio di informazioni rispetto alla situazione concorrenziale che si verrebbe a creare in assenza dello specifico scambio di informazioni. Affinché uno scambio di informazioni abbia effetti restrittivi sulla concorrenza ai sensi dell'articolo 101, paragrafo 1, deve sussistere la probabilità che esso abbia significativi effetti negativi su uno o più parametri di concorrenza, come il prezzo, la produzione, la qualità o la varietà del prodotto o l'innovazione.».

[28] Merita sottolineare come il diritto d'accesso ai documenti delle istituzioni dell'Unione europea non richieda la dimostrazione di un interesse specifico. Un tale regime risponde a un principio generale di trasparenza dell'azione amministrativa europea. Sul punto si veda M. Salvadori, *Il diritto di accesso all'informazione nell'ordinamento dell'Unione Europea*, in << http://www.evpsi.org/output>>.

[29] Cfr. B. Ponti, *Il patrimonio informativo pubblico come risorsa: i limiti del regime italiano di riutilizzo dei dati delle pubbliche amministrazioni*, in *Dir. pubbl.*, n. 3, 2007. L'autore evidenzia la supremazia (la 'signoria') delle norme interne riguardanti l'accesso su quelle europee in materia di riutilizzo.

simile contrasto giuridico appare tanto più chiaro se si considera la stretta implicazione – per non dire la sostanziale identità – tra i profili dell'accesso e del riutilizzo. Al riguardo, va rilevato come l'accesso alle Psi e il loro riutilizzo, pur individuando fasi distinte (per lo più in ragione della considerazione di una fase intermedia di acquisizione), vadano tuttavia trattati alla stregua di un concetto unitario in cui l'accesso alle Psi è funzionale al reimpiego delle stesse o – detto diversamente – il riutilizzo è la pacifica conseguenza dell'accesso perché ne è lo scopo. Alla luce di tale unitarietà, il diritto al riutilizzo delle informazioni del comparto pubblico si identifica con il diritto d'accesso alle stesse; e dunque il riutilizzo libero può ottenere un proprio spazio giuridico attraverso una modifica delle norme in materia di accesso[30]. Una tale prospettiva dovrebbe implicare, per la normativa dell'accesso, un qualche allargamento delle proprie maglie, con la riduzione dei casi in cui l'accesso resta escluso ovvero subordinato ai requisiti soggettivi di legittimazione, anche con la previsione della possibilità di riutilizzare singole informazioni estratte dai documenti. Con riguardo al nostro ordinamento, non va sottaciuto come la legge che disciplina l'accesso ai documenti amministrativi (l. n. 241/90) abbia adottato vincoli stringenti per la loro disponibilità, escludendo comunque l'accesso finalizzato al controllo generalizzato dell'operato delle pubbliche amministrazioni (art. 24, c. 3)[31]; in più, di tale norma non può non rilevarsi una qualche incoerenza con il riferimento al princìpio di trasparenza su cui – a dire della stessa legge – l'attività amministrativa dovrebbe reggersi (art. 1, c. 1 e art, 22, c. 2). Tutt'altro, dunque, che una "casa di vetro", per dirla con la metafora di Filippo Turati da egli utilizzata agli inizi del secolo scorso, e che pure è all'origine dei lavori che hanno portato alla stesura della legge n. 241/90[32].

---

[30] In tal senso ne parla, con vena ironica, S. Giacchetti, *Una nuova frontiera del diritto d'accesso: il «riutilizzo dell'informazione del settore pubblico» (Direttiva 2003/98/C.E.)*, in *Il Consiglio di Stato*, n. 5-6, 2004, 1249-1257: «Comunque sia, si finisce in buona sostanza col richiedere agli ordinamenti nazionali che, senza toccare le rispettive normative in materia d'accesso e riservatezza, creino al riutilizzo uno spazio che, in concreto, può essere ricavato solo modificando le rispettive normative in materia d'accesso e/o di riservatezza: il che è una sorta di quadratura del cerchio. Per i parlamenti nazionali dovrebbero aprirsi stimolanti spazi di enigmistica giuridica.». Al riguardo, va osservato come, invero, il legislatore europeo non sembra occuparsi di come la disciplina del riutilizzo venga recepita dagli stati membri, se cioè questa venga integrata nei regimi nazionali dell'accesso oppure venga adottata separatamente da essi.

[31] In tal senso cfr. G. Mancosu, *Trasparenza amministrativa e open data: un binomio in fase di rodaggio*, in *federalismi.it*, n. 17, 2012.

[32] Cfr. V. Sarcone, *Dalla «casa di vetro» alla «home page»: la «trasparenza amministrativa» nella legge 15/2009 e nel suo decreto attuativo (passando per la legge n. 69/2009)*, in *Amministrativ@mente*, n. 11, 2009, in particolare alla nota 11.

3.1. Evoluzione della disciplina europea dell'apertura e del riutilizzo delle Psi.

Nel corso del tempo, la prospettiva dell'*open (big) data* ha trovato inserimento in quel processo riformista del settore pubblico caratterizzato, tra l'altro, dall'obiettivo dell'introduzione, a scopo di efficienza, delle Ict nei processi interni e nei rapporti con il privato[33], e orientato a un modello pluralista e paritario piuttosto che bipolare e gerarchico[34]. Le politiche comunitarie in materia di riutilizzo dell'informazione del settore pubblico hanno introdotto, con la direttiva del 2003, l'istituto del riutilizzo libero (che non richiede, cioè, la dimostrazione di un particolare e legittimo interesse); passaggio, questo, che presuppone l'esistenza di una categoria di Psi per la quale non vi è una ragione di esclusione dall'accesso o di previsione di un accesso selettivo, e che ha aperto alla prospettiva di una disciplina del riutilizzo che potesse modificare quella dell'accesso o, comunque, coordinarsi con essa. Peraltro, l'esperienza di quasi un decennio ha messo in evidenza come solo alcuni stati membri abbiano provveduto in tal senso in occasione del recepimento della direttiva del 2003[35]; il che ha indotto il legislatore europeo a correggere il tiro stabilendo l'obbligo per gli stati membri di provvedere alla possibilità di riutilizzo di quella categoria di Psi, per così dire, «residuale» rispetto ai casi per i quali l'accesso è escluso o limitato. Un tale passaggio ha preso corpo con l'adozione della direttiva n. 37 del giugno 2013 che ha modificato quella del 2003[36], segnando una discontinuità nelle politiche del riutilizzo; discontinuità che riflette la volontà del legislatore dell'Unione di rimuovere le barriere che hanno impedito la valorizzazione del patrimonio informativo delle amministrazioni degli stati membri. Il diritto al riutilizzo delle Psi dunque si rafforza nel segno di un obbligo che ha reso il riuso esterno una condizione 'predefinita' (*by default*); i dati sono, cioè, in partenza riutilizzabili, fatti salvi i casi in cui l'accesso è escluso o limitato[37]. Condizione che, alla luce dei principi di apertura che sostengono il diritto al riutilizzo[38], può ricondursi pacificamente al più noto *open data by default*,

---

[33] Cfr. M. Pietrangelo, *Brevi note sul "coordinamento informativo informatico e statistico dei dati dell'amministrazione statale, regionale e locale"*, in *Informatica e diritto*, n. 1-2, 2004, 35-65; M. Bombardelli, *Informatica pubblica, e-government e sviluppo sostenibile*, in *Riv. Ital. Dir. Pubbl. Comunitario*, 2002, 991-1028, in particolare 999-1001.

[34] Con le parole di G. Arena, *Cittadini attivi*, Roma-Bari, Laterza, 2006.

[35] Come già rilevato dalla Commissione europea nel 2009 nella comunicazione sul riesame della direttiva del 2003. Al riguardo si veda Commissione europea, *Riutilizzo dell'informazione del settore pubblico*, cit.

[36] Cfr. direttiva 2013/37/UE, *che modifica la direttiva 2003/98/CE relativa al riutilizzo dell'informazione del settore pubblico*, in *GUUE*, L 175 del 27 giugno 2013, p. 1.

[37] Come chiaramente espresso nel considerando n. (8) della direttiva 2013/37/UE: «Occorre pertanto modificare la direttiva 2003/98/CE affinché stabilisca in modo chiaro l'obbligo per gli Stati membri di rendere riutilizzabili tutti i documenti *a meno che* l'accesso sia limitato o escluso ai sensi delle disposizioni nazionali sull'accesso ai documenti e fatte salve le altre eccezioni stabilite nella presente direttiva. Le modifiche apportate a opera della presente direttiva non cercano di definire o modificare i regimi di accesso all'interno degli Stati membri, che restano di responsabilità di questi ultimi.» (corsivo dell'autore).

[38] Si vedano, al riguardo, le considerazioni preliminari alla direttiva 2013/37/UE, in particolare i considerando

principio che, nello stesso periodo di adozione della direttiva europea, veniva consacrato dalla *G8 open data charter*, un documento di autoregolamentazione sottoscritto dai paesi del forum *G8*[39]. Merita anche sottolineare come, nell'introdurre il principio del riutilizzo *by default*, un siffatto quadro giuridico abbia ribaltato il rapporto di prevalenza tra l'interesse legato al riutilizzo libero delle PSI e gli interessi che, invece, ne escludono o ne limitano l'accesso, stabilendo la superiorità del primo rispetto agli altri. Il resto è una questione di attuazione. Sul piano pratico, il diritto al riutilizzo implica l'adozione, da parte degli stati membri, di modalità e strumenti idonei a favorire l'accesso della società civile alle PSI; in questa prospettiva, gli stessi paesi membri dovranno provvedere affinché le pubbliche amministrazioni individuino e rendano note e aperte le categorie di PSI destinate al riutilizzo generalizzato.

3.2. Cenni sui più recenti sviluppi in materia di apertura e riutilizzo delle PSI nell'ordinamento interno.

L'esperienza del nostro paese in materia di *openness* e riutilizzo delle PSI si avvia con il recepimento nel diritto interno della PSI *directive* ad opera del d. lgs. n. 36/2006[40]. Al riguardo, va osservato come, in tale occasione, il legislatore nazionale non si sia mostrato particolarmente illuminato sulle opportunità di un riutilizzo delle PSI a carattere generale, lasciando la sua adozione nella facoltà decisionale delle pubbliche amministrazioni; fanno eccezione le iniziative legislative di alcune regioni in tal senso lungimiranti, tra cui va menzionato l'esempio del Piemonte con la legge regionale n. 24/2011 in cui l'amministrazione regionale si è vincolata a garantire l'ampia libertà di accesso ai dati pubblici di cui è detentrice e il loro riutilizzo, attraverso la pubblicazione in formati aperti[41]. Insieme a queste esperienze merita richiamare anche la segnalazione al Governo e al Parlamento dell'Autorità garante della concorrenza e del mercato, in cui l'Antitrust sottolinea la necessità di alcuni interventi idonei a favorire lo sviluppo dei mercati legati al riutilizzo delle PSI; al riguardo, va menzionata, tra le altre, la proposta "*di trasformare in un obbligo l'attuale facoltà delle amministrazioni di consentire il riutilizzo delle informazioni in loro possesso.*"[42]. Sul fronte legislativo nazionale, il salto di qualità si registra con il decreto-legge n. 179 dell'ottobre 2012 (convertito in legge nel dicembre 2012)[43], in cui, oltre l'obbligo per le pubbliche amministrazioni di rendere noto il

n. (6), (20), (21) e (26)

[39] Si veda al riguardo <http://www.agid.gov.it/notizie/adottato-il-g8-open-data-charter>.

[40] Pubblicato in *G.U.* n. 37 del 14 febbraio 2006.

[41] All'iniziativa piemontese hanno fatto seguito quelle del Lazio, della Puglia e della Provincia autonoma di Trento.

[42] Cfr. AUTORITÀ GARANTE DELLA CONCORRENZA E DEL MERCATO, *Proposte di riforma concorrenziale ai fini della legge annuale per il mercato e la concorrenza anno 2013*, in *Boll.* n. 38/2012, 35.

[43] Cfr. il testo coordinato con la legge di conversione 17 dicembre 2012, n. 221, in *G.U.* n. 9 del 11 gennaio 2013, Suppl. ord. n. 4, in cui l'art. 9 modifica l'art. 52 del d.lgs. n. 82/2005 (*Codice dell'amministrazione digitale*).

catalogo dei dati (e dei metadati) destinati al riutilizzo libero, viene affermato il principio dell'apertura predeterminata; passaggio di cui va sottolineato il merito di aver anticipato la direttiva 2013/37/UE e l'iniziativa assunta in ambito *G8*. Un tale strumento giuridico ha stabilito l'apertura dei dati – e, per conseguenza, la possibilità del loro riutilizzo, alla luce dell'implicazione contenuta nel riscritto articolo 68, c. 3 del d.lgs. n. 82/2005 – anche nei casi in cui questi sono pubblicati senza la specificazione di una licenza[44]; l'assenza di licenza, dunque, non rappresenta una barriera alla possibilità di accesso e riutilizzo ma, anzi, conferisce ai dati lo *status* di patrimonio informativo pubblico riutilizzabile senza alcun vincolo.

Il processo normativo interno concernente l'apertura dei dati del settore pubblico si integra con le disposizioni che riordinano, in un testo unico, la disciplina in materia di pubblicità, trasparenza e diffusione delle informazioni da parte delle pubbliche amministrazioni. Il testo unico (d.lgs. n. 33/2013)[45] riconduce in seno al principio della trasparenza sia la pubblicità di dati, informazioni e documenti concernenti tutti gli aspetti della funzione pubblica sia la loro apertura onde agevolarne il riutilizzo che, in tale contesto, ha una finalità principalmente di controllo sociale dell'azione amministrativa; al riguardo, va precisato che le disposizioni del testo unico sulla trasparenza amministrativa sono limitate alle risorse conoscitive rilevanti sotto il profilo della trasparenza dell'azione amministrativa[46]. La previsione di prescrizioni sull'apertura delle Psi in un quadro di trasparenza appare coerente con quel principio di "accessibilità totale" che fu della legge n. 15/2009 (e puntualmente ripreso dal d.lgs. di attuazione n. 150/2009), e che il testo unico del 2013 ha riproposto in termini sostanzialmente analoghi. La portata rivoluzionaria del principio dell'accessibilità totale va ricondotta alla possibilità di conoscere dati, informazioni e documenti senza che le pubbliche amministrazioni possano frapporre ostacoli contrattuali (licenze), tecnici (formati), economici che, quanto meno, ne limiterebbero l'accesso e la possibilità del riutilizzo[47]; il che conferisce alla società civile quel contropotere democratico necessario a riequilibrare il rapporto con le pubbliche amministrazioni.

---

[44] L'adozione di una licenza da parte delle amministrazioni titolari dei dati deve essere comunque motivata in conformità alle linee guida nazionali definite dall'Agenzia per l'Italia digitale. Cfr. M. Ragone, *I dati aperti: l'innovazione a portata di cittadini, pubblica amministrazione, imprese*, in *Rivista degli infortuni e delle malattie professionali*, n. 3, 2012, 803-812.

[45] Cfr. d.lgs 14 marzo 2013, n. 33, *Riordino della disciplina in materia di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni*, in *G.U.*, n. 80 del 5 aprile 2013.

[46] Opportunamente elencate nell'articolato del d.lgs. n. 33/2013 (cfr. art. 12 e ss.).

[47] Sul punto si veda S. Toschei, *Accesso civico ed accesso ai documenti amministrativi, due volti del nuovo sistema amministrativo in Italia*, in *Comuni d'Italia*, vol. 50, n. 3, 2013, 9-23.

4. Le Ict nella prospettiva dell'accesso ai big data pubblici

Il ruolo dell'informazione e della conoscenza nell'esperienza umana è ben rappresentato dalle riflessioni di alcuni autori i quali, riferendosi alla comunicazione (funzione strumentale allo scambio di informazioni), hanno osservato come essa sia sempre stata una funzione necessaria e universale, connaturata all'essere umano[48]. Da ciò, ne consegue che la società dell'informazione e della conoscenza è sempre esistita se si considera che in una situazione sociale "non si può non comunicare"[49], e che queste risorse sono il contenuto della comunicazione. Il resto è una questione di progresso tecnologico e di evoluzione dei mezzi di comunicazione che, nel corso del tempo, hanno connotato diversamente la società dell'informazione.Al riguardo, merita sottolineare come l'avvento di internet – l'ultimo *medium* apparso in ordine temporale – abbia modificato le regole di circolazione dei contenuti con il superamento del modello di comunicazione verticale (che per lungo tempo ha segnato il primato della televisione tradizionale) e con la prospettiva che anche i singoli individui possono svolgere la funzione di 'emittenza'[50].Sotto questo aspetto, i siti informativi individuali e i *social media* sono esempi emblematici di un'evoluzione delle forme di diffusione dell'informazione e della conoscenza di cui non vanno sottaciute le implicazioni di *empowerment* della società civile e dunque di attenuazione del potere storicamente concentrato nei *media* tradizionali e nella sfera governativa[51]. L'esperienza quotidiana, poi, non fa altro che confermare il carattere di 'bene' di interesse generale dei contenuti informativi e conoscitivi perché la loro utilità si riferisce a un bisogno cognitivo innato nell'uomo che si estende a tutte le figure sociali (imprese, organizzazioni, istituzioni)[52]. Sotto questo aspetto, il valore dei contenuti sta nella loro capacità di ridurre l'incertezza e di concorrere alla formazione di nuova conoscenza con la quale i membri di una società possono migliorare i propri processi, dalle politiche governative (economiche, sociali, del lavoro) alle valutazioni dei consumatori sul profilo delle imprese (offerta, rispetto dell'ambiente, responsabilità sociale).
In tale prospettiva, il riutilizzo dei contenuti di fonte pubblica svolge un ruolo di primo

---

[48] Al riguardo, cfr. G.P. Caprettini, P. Ortoleva, *Introduzione*, in J.N. Jeanneney, *Storia dei media*, Roma, 1996, XI-XXI.

[49] È il primo assioma della comunicazione umana, formulato dallo psicologo e filosofo austriaco Paul Watzlawick e dagli studiosi del Mental Research Institute di Palo Alto (California). Sull'argomento si veda P.Watzlawick, J.H. Bravin, D.D Jackson, *Pragmatica della comunicazione umana*, Roma, Astrolabio, 1971.

[50] In tal senso V. Zeno-Zencovich, *La libertà d'espressione. Media, mercato, potere nella società dell'informazione*, Bologna, Il Mulino, 2004, p. 125 ss. Si veda anche E. Rosati, G. Sartor, *Social networks e responsabilità del provider*, in *EUI LAW*; n. 5, 2012.

[51] Il caso *Wikileaks* – nel bene e nel male – è la dimostrazione più chiara di una tale emancipazione.

[52] In tal senso, si veda G.O. Longo, *Il poliedrico mondo dell'informazione*, in *Mondo digitale*, n. 2, giugno 2006, 3. Nel suo lavoro l'autore esordisce ponendo l'informazione alla base di ogni attività umana, sottolineando come "[…] tutta l'evoluzione, prima biologica e poi sociale e culturale, è stata contrassegnata da scambi d'informazione sempre più intensi e diffusi.".

piano, rappresentando una condizione essenziale per le scelte private, in particolare per le decisioni degli operatori economici. Al riguardo, va sottolineato come le politiche comunitarie in materia di riuso delle Psi abbiano posto particolare enfasi sull'impiego di queste risorse allargato alla società civile (per scopi diversi da quelli connessi alla funzione di servizio pubblico), avendone intuito gli effetti sull'attività economica e dunque sulla competitività dei paesi membri. A partire dal libro verde del 1998[53], dal lato del regolatore europeo si sono percepite aspettative di crescita economica, di creazione di posti di lavoro, di concorrenza sul mercato interno, legate alla visione che i contenuti di provenienza pubblica avrebbero dovuto essere accessibili alle imprese nella prospettiva che queste potessero fornire nuovi prodotti e servizi[54]. E, invero, sotto questo aspetto, va osservato come l'attività di nascenti imprese innovative – come nel caso di *start up* che producono applicazioni *software* per dispositivi mobili – sia fortemente dipendente dalla possibilità di attingere alle risorse informative e conoscitive di fonte pubblica. Si pensi, in tal senso, ai contenuti meteorologici e a quelli geografici che rappresentano un *input* essenziale per la fornitura di servizi a valore aggiunto; un opportuno trattamento di queste risorse può fornire, ad esempio, indicazioni sull'*appeal* turistico di un'area geografica o previsioni utili per il comparto agricolo. Analoghe considerazioni valgono, ad esempio, sul fronte dell'innovazione civica, là dove l'"intelligenza urbana" (*smart city*) si consegue con lo sfruttamento dei *big data* delle amministrazioni interessate (locali e centrali)[55].

In tutto questo, la parte che le Ict sono chiamate a fare è tutt'altro che marginale se si considera che, sotto il profilo operativo, la prospettiva è, da un lato, la gestione di masse di dati pubblici equiparabili a strutture di *big data* e, dall'altro, il trasporto delle stesse che richiede la disponibilità di reti con capacità adeguate. Sul fronte europeo, l'introduzione delle Ict nei processi dei settori pubblico e privato rappresenta una strategia ben nota per le sue implicazioni di efficienza; sul punto, merita ricordare come le politiche della società

---

[53] Cfr. Commissione europea, *L'informazione del settore pubblico: una risorsa fondamentale per l'Europa. Libro verde sull'informazione del settore pubblico nella società dell'informazione*, (COM(1998) 585). Invero, vanno ricordate anche le linee direttrici sulle sinergie informative tra pubblico e privato del 1989. Il riferimento al libro verde, con cui a quasi dieci anni di distanza la Commissione europea tornò sul tema, appare tuttavia più pertinente, perché è da allora che la politica dell'apertura delle Psi ai riutilizzi esterni ha posto le basi per l'adozione della direttiva 2003/98/CE.

[54] Cfr. U. Fantigrossi, *I dati pubblici tra Stato e mercato*, in *Amministrare*, n. 1-2, 2007, 277-294.

[55] Cfr. Evpsi, *Libro bianco per il riutilizzo dell'informazione del settore pubblico*, 2012, reperibile all'indirizzo <http://www.evpsi.org/output> (in cui sono indicati gli autori che, a vario titolo, hanno contribuito alla pubblicazione del libro bianco); Si veda anche G. Cimpanelli, *I big data sono il futuro del turismo: noi li usiamo così*, reperibile all'indirizzo <http://www.economyup.it/startup/1479i-big-data-sono-il-futuro-del-turismo-noi-li-usiamocosi.htm>, in cui si illustra l'esperienza di Travel Appeal, un'impresa che, con l'ausilio di un *software*, analizza il *sentiment* e la *reputation* di possibili destinazioni turistiche. Sull'innovazione civica si veda A. Paparo, *Anticipare i bisogni delle persone con i big data: così si crea una smart city*, all'indirizzo <http://www.economyup.it/innovazione/975_anticipare-i-bisogni-delle-persone-con-i-big-data-cosi-si-crea-una-smart-city.htm>; Cfr. anche Key4biz, *Big data city: volume, velocità e varietà dei dati saranno le tre variabili della futura crescita economica*, reperibile all'indirizzo <http://www.key4biz.it/Smart-City-2013-01-Big-Data-City-Dati-Ict-Smart-City-Smart-Economy-Energia-Ambiente-Tecnologia-Pulita-215182/>.

dell'informazione e della conoscenza, a partire dal rapporto Bangemann del 1994, si siano concentrate su queste risorse per ridefinire le dinamiche sociali – di cui il commercio e il governo elettronico costituiscono i principali capisaldi[56], [57] – in una prospettiva di competitività e di benessere.

Gli aspetti gestionali dei contenuti sono rimessi all'impiego di tecnologie di trattamento individuate, in astratto, dal *software* (che la letteratura tecnica spesso sintetizza con il termine It, *information technologies*); una tale risorsa, che realizza l'automazione dell'elaborazione, è un tratto decisamente significativo della società dell'informazione; l'esempio di 'Wikipedia' è indicativo se si considera che, sotto il profilo tecnico, la sua principale funzione – la condivisione di informazioni e conoscenze – è supportata da una famiglia di *software* denominata *wiki*[58]. Non va peraltro sottaciuto che il contributo delle It ha anche una valenza cognitiva, individuabile nella capacità di ridurre quei limiti della razionalità umana a cui faceva riferimento Herbert Simon negli anni Cinquanta del secolo scorso con la sua teoria della razionalità limitata[59]; sotto questo aspetto, l'It può sopperire, in parte, all' "algoritmo umano" correggendo taluni errori cognitivi che i decisori solitamente commettono quando, nelle loro scelte, ricorrono a regole pratiche (*heuristics*)[60]. Il fenomeno *big data* pone tuttavia all'innovazione tecnologica nuove sfide,

---

[56] Le politiche comunitarie sul commercio elettronico possono essere fatte risalire a una comunicazione della Commissione dell'aprile 1997 che ha rappresentato la base di riferimento della direttiva sul commercio elettronico adottata nel giugno del 2000. Al riguardo si veda Commissione delle comunità europee, *Un'iniziativa europea in materia di commercio elettronico*, 16 aprile 1997, (COM(97) 157). Come è noto, le dinamiche del commercio elettronico vanno ricondotte a fattori di diversa natura, regolamentari, tecnico-economici (investimenti in reti *broadband*, prezzi), tecnologici (misure tecniche di sicurezza), psicologici (fiducia). Per una disamina dell'evoluzione del commercio elettronico si veda il saggio di A. Grando, *Commercio elettronico: tra crisi e ripresa*, in *Consumatori, diritti e mercato*, n. 3, 2012, 114-122.

[57] Cfr. E. Liikanen, *L'e-Government e l'Unione Europea*, in *European Journal for the informatics professional*, vol. IV, n. 2, 2003 (reperibile all'indirizzo <http://www.cepis.org/upgrade/index.jsp?p=0&n=2178&a=3089>). Nel nostro paese il modello del governo elettronico è un elemento centrale del progetto di riforma della pubblica amministrazione che si connota sotto il profilo dell'accesso alle informazioni e ai servizi attraverso la Rete. La prospettiva riformista dell'*e-government* lascia dunque ben sperare sugli obiettivi di *spending review* e sui recuperi di produttività del settore pubblico che influenzano direttamente la produzione interna; ma fa anche confidare sull'efficienza della fornitura dei servizi pubblici, nell'ambito dei quali vanno annoverati anche i servizi legati all'apertura alle Psi, con effetti sull'attività economica degli operatori privati e dunque sul Pil. Su questi argomenti cfr. Cfr. M. Calise, R. De Rosa, *Il governo elettronico: visioni, primi risultati e un'agenda di ricerca*, in *Rivista italiana di scienza politica*, n. 2, 2003, 257-284; M. Bombardelli, *Informatica pubblica, e-government e sviluppo sostenibile*, in *Riv. Ital. Dir. Pubbl. Comunitario*, 2002, 991-1028; R. De Rosa, *Il parlamento italiano alla prova tecnologica*, in *Politica del diritto*, n. 3, 2010, 545-569. Sugli effetti delle Ict sulla *spending review* si veda l'interessante libro bianco di Microsoft, Netics, *La comunicazione digitale al servizio della Spending Review*, febbraio 2013.

[58] Cfr. L. Paccagnella, *La gestione della conoscenza nella società dell'informazione: il caso di Wikipedia*, in *Rassegna italiana di sociologia*, n. 4, 2007, 653-680;

[59] Cfr. H.A. Simon, *Administrative behavior*, New York, Macmillan, 1947; P. Legrenzi, *Razionalità: economia e psicologia*, in *Rivista italiana degli economisti*, n. 1, 2005, 43-56.

[60] Sul tema cfr. G. Masino, *Nuove tecnologie per le decisioni: una riflessione critica*, IV Workshop dei docenti e ricercatori di organizzazione aziendale, Firenze, 13-14 febbraio 2003; G. Olimpo, *Società della conoscen-*

richiedendo alle IT caratteristiche adeguate sotto i profili della dimensione, della velocità del trattamento e della capacità di analisi (quest'ultima finalizzata alla generazione di un valore).

Il trasporto dei *big data* è affidato alle reti di telecomunicazioni che, in senso lato, rappresentano l'altra componente delle ICT (le *communication technologies*). La capacità delle reti va pertanto opportunamente dimensionata nella prospettiva di flussi di traffico elevati a cui concorrono fenomeni come il *cloud computing*, i *social network*, nonché i servizi pubblici innovativi[61]. Le aspettative dell'Europa, dunque, sono riposte nella realizzazione di reti di "nuova generazione", idonee a supportare sia il trasferimento di notevoli quantità di contenuti sia la prestazione di servizi che integrano nuove utilità; condizioni, queste, che nella prospettiva dell'Unione, contribuiscono al principale obiettivo economico rappresentato dal mercato unico[62]. Peraltro, sappiamo come le politiche nazionali di promozione delle reti *broadband* siano estremamente eterogenee e non ancora conformi agli obiettivi definiti dall'agenda digitale europea[63]. Su questo versante, specie nel nostro paese, si intersecano questioni rilevanti, a cominciare dalla capacità di cui dovrebbero essere dotate le linee d'utente, la cui soglia minima ipotizzata

za, educazione, tecnologia, in *Tecnologie didattiche*, vol. 18, n. 2, 2010, 4-16, in cui, con riguardo ai processi educativi, l'autore osserva che le tecnologie digitali "possono assumere il significato di vere e proprie tecnologie *cognitive* capaci di promuovere nuove forme di organizzazione del pensiero, nuovi modi di apprendimento e nuove forme di comunicazione e collaborazione interpersonale."; M. PRENSKY, *H. sapiens digitale: dagli immigrati digitali e nativi digitali alla saggezza digitale*, in *Tecnologie didattiche*, vol. 18, n. 2, 2010, 17-24. Nondimeno, la funzione elaborativa dell'algoritmo umano ha una sua peculiarità, comprendendo percezioni, creatività e capacità combinatorie degli stimoli informativi e conoscitivi che non sono rimpiazzabili dalla tecnologia. Su questo punto si veda R. LEONI (a cura di), *Competenze acquisite, competenze richieste e competenze espresse*, Milano, Franco Angeli, 2006, 20.

[61] I fornitori di servizi di *computing* spesso trasferiscono i dati dei propri utenti all'interno della 'nuvola' sia per ottimizzare l'uso delle risorse *hardware* sia in occasione di duplicazioni effettuate per scopi di sicurezza. Si veda, al riguardo, COMMISSIONE EUROPEA, *Sfruttare il potenziale del cloud computing in Europa*, 27 settembre 2012 (COM(2012) 529). Sul fronte dei servizi pubblici, vanno segnalati gli esempi dei servizi sanitari e dell'istruzione la cui connotazione tecnologica contempla l'integrazione di contenuti, l'interattività audiovisiva e altre funzionalità che, nel corso del tempo, dovrebbero determinare il superamento degli analoghi servizi prestati nelle modalità tradizionali (*off line*). Con riguardo alla fornitura di servizi pubblici in rete si veda D. ARDUINI, S. NEPI, *Importanza delle infrastrutture a banda larga per la diffusione dell'e-Government*, in *Argomenti*, n. 15, 2005, 101-125.

[62] Cfr. COMMISSIONE EUROPEA, *Agenda digitale per l'Europa - Le tecnologie digitali come motore della crescita europea*, 18 dicembre 2012 (COM(2012) 784); COMMISSIONE DELLE COMUNITÀ EUROPEE, *"i2010 – Una società europea dell'informazione per la crescita e l'occupazione"*, 1 giugno 2005 (COM(2005) 229); COMMISSIONE DELLE COMUNITÀ EUROPEE, *eEurope 2002: un quadro normativo comunitario per la valorizzazione delle informazioni del settore pubblico*, 23 ottobre 2001 (COM(2001) 607); COMMISSIONE EUROPEA, *L'informazione del settore pubblico: una risorsa fondamentale per l'Europa*, cit. In letteratura si veda M. RAGONE, F. MINAZZI, *La dicotomia tra trasparenza e dati aperti*, in *Diritto mercato tecnologia*, n. 2, 2013, 89-100, in particolare 93.

[63] Sul punto cfr. N. IACONO, *Banda larga in Europa: mancano i piani*, marzo 2014, all'indirizzo <http://www.agendadigitale.eu/infrastrutture/741_banda-larga-in-europa-mancano-i-piani.htm>, in cui l'autore sottolinea come non tutti gli stati membri abbiano definito piani di sviluppo della banda larga come previsto dall'agenda digitale europea.

dall'agenda digitale europea si colloca al livello di 30 Mbit/s[64], a cui si aggiungono fattori (il *digital divide*, l'utilità percepita dal lato della domanda) che influenzano gli investimenti. Con riguardo a quest'ultimo aspetto, va altresì osservato che i progetti di *next generation network* implicano notevoli finanziamenti la cui disponibilità, dal lato del settore privato, appare decisamente incerta alla luce di rischi valutati eccessivi in rapporto al quadro economico generale; in altre parole, la crisi internazionale ha determinato incertezza sulla domanda e, conseguentemente, sul ritorno degli investimenti. A ciò si aggiungano i vincoli regolatori che gravano sulle imprese dominanti sulle quali tuttavia i governi degli stati membri confidano, essendo le più accreditate in fatto di investimenti. Su questo punto, merita sottolineare come, al di là degli impedimenti legati allo scenario economico di contorno, il principio della neutralità tecnologica su cui si fonda il quadro normativo dell'accesso alle reti – vale a dire, l'adozione di regole indipendenti dalla tecnologia – sia tutt'altro che incoraggiante per le iniziative economiche private, in particolare per quelle poste in essere da operatori con significativo potere di mercato; aspetto, questo, a cui la Commissione europea ha tentato di porre rimedio con la previsione di un rendimento del capitale investito che tenga conto degli eventuali rischi supplementari a cui andrebbe incontro l'operatore dominante[65], ma che non sembra abbia dispiegato effetti incentivanti, almeno nel nostro paese. Soluzioni alternative al *risk premium* sono rappresentate da politiche pubbliche nazionali di sostegno agli investimenti (*partnership* tra pubblico e privato, incentivi fiscali, accesso al credito agevolato, programmi di finanziamento), a cui andrebbero affiancati opportuni interventi sul lato della domanda. Va peraltro sottolineato come le risorse pubbliche per queste iniziative siano limitate alla luce di un quadro economico europeo ancora sostanzialmente critico e considerando la necessità delle politiche nazionali di indirizzare tali risorse anche verso altre aree di intervento (scuola, *welfare*, ammortizzatori sociali, infrastrutture pubbliche). In questo scenario, il settore privato deve poter contare anche su risorse economiche di fonte europea (come i fondi associati alla politica di coesione[66]) che, oltre a sostenerne gli investimenti, possano dare credibilità ai progetti di costruzione delle reti di nuova generazione e attrarre ulteriori capitali privati e pubblici.

Le Ict sono risorse che abilitano l'elaborazione e la diffusione delle informazioni da cui originano i processi di condivisione delle conoscenze. La prospettiva di poter attingere a un bacino cognitivo generato dall'applicazione delle Ict ai *big data* (e rigenerato dagli scambi in rete), ha fatto intravedere un orizzonte di crescita sociale che già Karl Marx

---

[64] Commissione europea, *Un'agenda digitale europea*, 26 agosto 2010, COM(2010) 245 definitivo/2.

[65] Si veda, a tal riguardo, Commissione europea, Raccomandazione 2010/572/UE, *relativa all'accesso regolamentato alle reti di accesso di nuova generazione (NGA)*, in *GUUE*, n. L 251, del 25 settembre 2010, p. 35.

[66] La politica di coesione è la principale politica di investimento dell'Unione europea. Tra i suoi obiettivi prioritari va segnalato il miglioramento dell'accesso alle tecnologie dell'informazione e della comunicazione (obiettivo banda larga). Al riguardo, si vedano i regolamenti per i fondi strutturali e di investimento europei 2014-2020 , reperibili all'indirizzo <http://ec.europa.eu/regional_policy/information/legislation/index_it.cfm>.

aveva intuito con le sue riflessioni a proposito del *general intellect*[67], e che Pierre Levy e Derrick de Kerckhove hanno individuato rispettivamente nell'intelligenza collettiva e nell'intelligenza connettiva[68]. Il *software* e le reti, dunque, hanno assunto un ruolo di primo piano nell'economia della conoscenza, essendo l'origine di un sistema cognitivo (un'intelligenza) risultante dal coordinamento di conoscenze «digitali» distribuite e connesse[69], su cui sono riposte aspettative di innovazione e di crescita economica. Gli investimenti nelle Ict – e, in particolare, nelle reti a elevata capacità – vanno pertanto ricondotti a strategie anti-crisi, funzionali alla ripresa economica di un paese e alla sua competitività internazionale; tutt'altro, dunque, che un semplice intervento di adeguamento tecnologico subordinato alla disponibilità di risorse. In questa prospettiva, i governi dovrebbero modificare la scala delle priorità a favore delle rispettive agende digitali.

5. *Big data* e implicazioni di potere.

Alle caratteristiche virtuose dell'utilizzo (e del riutilizzo) dei *big data* si contrappone tuttavia la prospettiva di ricadute sociali, in particolare nel caso in cui entrano in gioco interessi che implicano il controllo dei comportamenti di persone e aziende. Al riguardo, va osservato che la formazione e la gestione di simili strutture non è una prerogativa generalizzata essendo circoscritta a poche grandi imprese operanti, per lo più, attraverso internet, le cui capacità di raccolta sono tali da coprire quasi tutto il traffico *web*[70] e da determinarne una posizione nell'ecosistema digitale che Bauman e Lyon hanno definito di "sesto potere"[71]. L'esperienza della società *post*-industriale, a partire dal progetto 'Echelon' degli anni sessanta fino al più recente 'datagate', dimostra come questa capacità possa essere esplicata anche da enti pubblici o governativi attraverso strategie di sorveglianza

---

[67] Cfr. K Marx, *Lineamenti fondamentali della critica dell'economia politica*, vol. II, Firenze, La Nuova Italia, 1978. Su questo punto si veda anche C. Formenti, *Incantati dalla rete. Immaginari, utopie e conflitti nell'epoca di Internet*, Milano, 2000, 72, in cui l'autore osserva come l'accostamento (di Marx) della fabbrica a un organismo dotato di una propria intelligenza (*general intellect*) possa aver anticipato l'analogo fenomeno in rete.

[68] Cfr. P. Levy, *L'intelligenza collettiva. Per un'antropologia del cyberspazio*, Milano, Feltrinelli, 2002; D. De Kerckhove, *Connected intelligence: the arrival of the web society*, Toronto, Somerville House, 1997. Si veda anche F. Introini, *Comunicazione come partecipazione. Tecnologia, rete e mutamento socio-politico*, Milano, Vita e Pensiero, 2007.

[69] Cfr. E. Rullani, *Economia delle reti: l'evoluzione del capitalismo di piccola impresa e del «made in Italy»*, in *Economia e politica industriale,* n. 4, 2010, 141-165. L'autore definisce le reti (in senso lato) come "moltiplicatori cognitivi". Grazie alle reti, una conoscenza può essere trasferita a più operatori a un costo pressoché nullo; e ciascuno di questi può generare un valore addizionale (nuova conoscenza).

[70] Sul punto si veda G. Ziccardi, *I flussi d'informazione digitale e la loro sicurezza nel panorama geopolitico attuale*, luglio 2014, all'indirizzo <http://www.treccani.it/geopolitico/saggi/2014/i-flussi-d-informazione-digitale-e-la-loro-sicurezza-nel-panorama-geopolitico-attuale.html>.

[71] Cfr. Z. Bauman, D. Lyon, *Sesto potere. La sorveglianza nella modernità liquida*, Roma, Laterza, 2014.

(intercettazioni delle comunicazioni, individuazione dei percorsi effettuati in rete, trattamenti che conducono alla re-identificazione di dati anonimi[72]) poste in essere anche con il supporto degli operatori del settore delle ICT[73]. Simili condotte pongono seri interrogativi in tema di libertà e rispetto dei diritti fondamentali là dove, pur invocando le ragioni della sicurezza nazionale e della lotta al terrorismo e al *cyber crime*, vanno oltre i limiti imposti dal principio di proporzionalità. Espressioni di potere riconducibili al possesso di grandi insiemi di contenuti sono, altresì, rinvenibili nei comportamenti assunti dalle grandi imprese consistenti nella costruzione dei profili dei consumatori – attività spesso effettuate a loro insaputa – la cui giustificazione si rifà alla necessità di conformare i prodotti e i servizi alle utilità da questi ricercate.

5.1. L'esperienza europea (in particolare, la dichiarazione di invalidità della direttiva c.d. data retention).

Sul fronte europeo, le esigenze di sicurezza acuitesi dopo l'11 settembre 2001 hanno spinto gli stati membri a introdurre nei loro ordinamenti norme concernenti l'acquisizione e la custodia dei predetti dati. Al riguardo, non va sottaciuto come tali norme abbiano favorito la formazione di *big data* alla luce della possibilità di una loro applicazione indifferenziata alla popolazione degli utenti e di una conservazione dei dati raccolti per periodi prolungati. A queste iniziative ha fatto seguito – anche sulla scia degli attentati di Madrid (marzo 2004) e di Londra (luglio 2005) – l'adozione della direttiva 2006/24/CE sulla conservazione dei dati inerenti la fornitura di servizi di telecomunicazioni[74]. Il provvedimento riflette l'esigenza del legislatore europeo di definire un quadro normativo comune, idoneo a eliminare gli ostacoli al mercato interno derivanti dalla prospettiva che gli operatori destinatari degli obblighi di conservazione avrebbero dovuto assecondare esigenze degli stati membri diverse sotto il profilo della tipologia dei dati e delle condizioni di *retention*[75]. Sappiamo, tuttavia, come un siffatto provvedimento sia stato posto in discussione, già al tempo della sua stessa proposta[76], da alcuni organi istituzionali comunitari[77] che, con toni più o meno

---

[72] Sulla re-identificazione dei dati anonimi si veda M. Viola de Azevedo Cunha, D. Doneda, N. Andrade, *La re-identificazione dei dati anonimi e il trattamento dei dati personali per ulteriore finalità: sfide alla privacy*, in *Ciberspazio e diritto*, vol. 11, n. 4, 2010, 641-655.

[73] Sul punto, si veda E. Falletti, *La lotta al terrorismo e i limiti della violazione della sfera privata individuale: il caso delle intercettazioni abusive di massa*, in *Diritto dell'internet*. n. 1, 2007, 54 ss.

[74] Pubblicata in *GUUE*, L 105 del 13 aprile 2006, 54-63.

[75] Cfr. M. Gialuz, *La cooperazione informativa quale motore del sistema europeo di sicurezza*, in F. Peroni, M. Gialuz (a cura di), *Cooperazione informativa e giustizia penale nell'Unione europea*, Trieste, 2009, 15 ss.

[76] Si veda, al riguardo, Commissione delle comunità europee, *Proposta di direttiva del Parlamento europeo e del Consiglio riguardante la conservazione di dati trattati nell'ambito della fornitura di servizi pubblici di comunicazione elettronica e che modifica la direttiva 2002/58/CE*, Bruxelles, 21 settembre 2005, reperibile in rete all'indirizzo <http://eur-lex.europa.eu/legal-content/IT/TXT/DOC/?uri=CELEX:52005PC0438&rid=1>.

[77] Il riferimento è al Comitato economico e sociale europeo, al garante europeo della protezione dei dati e al Gruppo di lavoro art. 29, che hanno criticato la proposta di direttiva sulla conservazione dei dati. Al ri-

aspri, ne hanno sottolineato l'eccessiva ingerenza nella vita privata degli utenti. A ciò vanno aggiunte le domande di pronuncia pregiudiziale proposte dopo l'adozione della direttiva del 2006 dalla *High Court* irlandese e dalla Corte costituzionale austriaca alla Corte di giustizia dell'Unione europea, riguardanti la compatibilità della citata direttiva con la Carta dei diritti fondamentali dell'Unione europea; le predette domande riflettevano evidentemente quegli stessi dubbi, emersi durante i lavori preparatori, sulla conservazione di una quantità ampia di dati (raccolti su un numero illimitato di soggetti, prescindendo da criteri selettivi) per tempi particolarmente lunghi[78]. Il parere dell'avvocato generale della Corte di giustizia dell'Unione europea, reso nel dicembre 2013[79], e la sentenza con cui la stessa Corte, riunendo le due cause, nell'aprile 2014 ha dichiarato l'invalidità della direttiva del 2006[80], hanno fatto il resto, evidenziando i profili di pregiudizio della privacy degli utenti interessati; al riguardo, è stato osservato come oltre alla possibilità di ricostruire l'identità degli individui e molti aspetti della loro esistenza, la direttiva non abbia previsto misure atte a contrastare possibili trattamenti abusivi e a garantire la conservazione dei dati all'interno dell'Unione. Sul lato della dottrina è stato osservato come la *law in action* del caso *data retention* possa rappresentare un modello di tutela dei diritti fondamentali da

guardo, si vedano: *Parere del Comitato economico e sociale europeo in merito alla Proposta di direttiva del Parlamento europeo e del Consiglio riguardante la conservazione di dati trattati nell'ambito della fornitura di servizi pubblici di comunicazione elettronica e che modifica la direttiva 2002/58/CE,* in *GUUE*, C 69, del 21 marzo 2006, p. 16; Garante europeo della protezione dei dati, *Parere del garante europeo della protezione dei dati (GEPD) sulla proposta di direttiva del Parlamento europeo e del Consiglio relativa alla conservazione dei dati trattati in relazione alla fornitura di servizi di comunicazione elettronica pubblici e recante modifica della direttiva 2002/58/CE*, in *GUUE*, C 298, del 29 novembre 2005, p. 1; articolo 29 - Gruppo per la tutela dei dati personali, *Parere 4/2005 sulla proposta di direttiva del Parlamento europeo e del Consiglio riguardante la conservazione di dati trattati nell'ambito della fornitura di servizi pubblici di comunicazione elettronica e che modifica la direttiva 2002/58/CE (COM(2005)438 definitivo del 21.9.2005)*, all'indirizzo <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion- recommendation/index_en.htm#h2-10>. Rileva osservare come, all'indomani dell'approvazione della direttiva *data retention*, il Gruppo art. 29 sia tornato sulle riserve espresse nel parere 4/2005. Si veda, al riguardo, Gruppo di lavoro protezione dati articolo 29, *Parere 3/2006 sulla direttiva 2006/24/CE del Parlamento europeo e del Consiglio riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE*, all'indirizzo <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm#h2-10>

[78] Cfr. M. Messina; *La corte di giustizia UE si pronuncia sulla proporzionalità delle misure in materia di conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica e ne dichiara la loro invalidità*, in *Ordine internazionale e diritti umani*, n. 2, 2014, 396-401. Si veda anche O. Pollicino, *Internet nella giurisprudenza delle Corti europee: prove di dialogo?*, in *Forum di quaderni costituzionali*, <http://www.forumcostituzionale.it/site/ content/view/3/3/#p>.

[79] Conclusioni dell'Avvocato Generale Cruz Villalòn del 12 dicembre 2013 nella causa C-293/12 *Digital Rights Ireland Ltd v The Minister for Communications, Marine and Natural Resources The Minister for Justice, Equality and Law Reform The Commissioner of the Garda Síochána Ireland and The Attorney General*.

[80] Corte di giustizia dell'Unione europea, cause riunite C-293/2012 e C-594/12, *Digital Rights Ireland Ltd*, *Seitlinger e altri*, in *GUUE*, C 175, del 10 giugno 2014, 6 (testo completo della sentenza disponibile all'indirizzo < http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang =IT>).

situazioni di sorveglianza che risultano ingiustificate nella misura in cui vanno oltre i limiti posti dal principio di proporzionalità, come stabilito nella Carta dei diritti fondamentali dell'Unione europea (art. 52, par. 1)[81]. La sentenza della Corte ha posto le basi per la riscrittura di una direttiva che possa riequilibrare gli interessi in gioco che si delineano con la conservazione dei *big data* (sicurezza degli stati membri e privacy). L'incidenza di un tale (eventuale) strumento di regolazione – sia dei comportamenti di sorveglianza delle autorità nazionali sia delle posizioni di potere degli operatori incaricati dalle autorità medesime – riposa evidentemente sulla prospettiva di una revisione delle misure adottate per la conservazione e di procedure che contemplano l'invio di informazioni da parte degli Stati membri alla Commissione europea (notifiche, relazioni).

5.2. Implicazioni antitrust del trattamento dei *big data*

I contenuti rappresentati da dati, informazioni e conoscenze costituiscono per le imprese un fattore di competitività essenziale; le condizioni di accesso a queste risorse, dunque, contribuiscono a determinare il profilo del mercato. Sotto questo aspetto, va osservato come la concentrazione di grandi *database* in poche mani possa determinare strutture oligopolistiche o, comunque, possa indicare la presenza sul mercato di figure dominanti. Simili profili, se pure non sono di per sé stessi contrari alle regole della concorrenza, costituiscono tuttavia i presupposti di comportamenti restrittivi del gioco concorrenziale che possono esplicarsi, tra l'altro, attraverso il trattamento dei contenuti. In questa prospettiva, prende corpo la valutazione della rilevanza *antitrust* di taluni trattamenti dei *big data*, non essendo escluso che questi possano ostacolare ingiustificatamente la concorrenza. Una questione similare è stata posta dalla Commissione europea, in particolare con riguardo agli effetti sulle dinamiche concorrenziali dell'utilizzo di dati personali; nello *speech* del 26 novembre 2012 l'allora commissario europeo per le politiche della concorrenza, Joaquin Almunia, ha sottolineato come un'impresa potrebbe utilizzare i dati sulle abitudini di consumo dei propri clienti per ottenere un vantaggio sui concorrenti[82]. Seguendo questa traccia, la lente d'ingrandimento dell'antitrust potrebbe posarsi sui casi in cui il titolare del trattamento veste i panni di un *player* dominante e, in particolare, laddove i trattamenti diversi da quelli necessari (spesso effettuati senza il consenso degli interessati) rafforzano il suo potere di mercato restringendo la concorrenza. Partendo da questa premessa, le autorità garanti della concorrenza, dovrebbero poter valutare se una

---

[81] Cfr. V. Scalia, *Criminalità informatica vs diritto alla riservatezza e protezione dei dati personali. I legislatori (europeo e nazionale) alla ricerca del giusto punto di equilibrio nell'epoca della globalizzazione digitale*, in Aa.Vv, *Diritto alla privacy e trattamento automatizzato dei dati fra diritto civile, diritto penale e diritto internazionale ed europeo*, Università di Catania, 2014, 24-41. L'autore sottolinea il ruolo di controllo del rispetto dei diritti fondamentali da parte della Corte di giustizia dell'Unione europea (v., in particolare, p. 28).

[82] Cfr. J. Almunia, *Competition an personal data protection*, speech/12/860, 26 novembre 2012, reperibile all'indirizzo < http://europa.eu/rapid/press-release_SPEECH-12-860_en.htm>: "a single dominant company could of course think to infringe privacy laws to gain an advantage over its competitors".

determinata elaborazione di dati è suscettibile di integrare una violazione dell'articolo 102 del trattato sul funzionamento dell'Unione europea. Più in generale, va sottolineato come nell'ambito dei trattamenti effettuati da un soggetto dominante possano annidarsi pratiche abusive, rilevanti sia sul piano della *data protection* sia per gli aspetti *antitrust*. In questa prospettiva, sembra opportuno che le autorità di garanzia interessate (della privacy e della concorrenza) possano coordinarsi per valutare i casi in cui i due profili si intersecano. Esempi che, in tal senso, vanno tenuti d'occhio sono rappresentati dall'utilizzo dei dati di consumo di servizi pubblici liberalizzati – in particolare, servizi di telecomunicazioni – per scopi di trattenimento degli utenti ovvero per il recupero di quelli passati ad altro operatore. Esemplare in tal senso è il caso *antitrust "Sfruttamento di informazioni commerciali privilegiate"*; il procedimento, avviato nell'ottobre del 2007 a carico della società Telecom Italia, aveva lo scopo di accertare il carattere abusivo dello sfruttamento della propria posizione dominante, attuato attraverso comportamenti connessi all'uso di informazioni sul traffico degli utenti (procedimento chiuso dall'autorità senza accertare l'infrazione in ragione degli impegni assunti dall'operatore di telecomunicazioni ai sensi dell'articolo 14-*ter* della legge n. 287/90)[83].

Altro caso prospettato dalla Commissione europea è quello del trasferimento dei dati di persone e aziende che intendono cambiare operatore. Si pensi, al riguardo, agli utenti di un *social network* dominante che vorrebbero portare altrove i contenuti che compongono il loro profilo; in questa eventualità, il trattamento dei dati consistente nella loro conservazione di lungo periodo appare quanto meno critico dal punto di vista *antitrust*, potendo configurare un ostacolo al cambiamento di natura abusiva. Sotto il profilo tecnico, non va sottaciuto come simili comportamenti di *lock-in* siano facilitati da una scarsa interoperabilità tra le piattaforme e dalla non neutralità dei formati dei dati[84], e dunque dal permanere di soluzioni tecnologiche proprietarie e differenziate che determinano condizioni di dipendenza degli utenti dagli operatori di origine[85]. Merita osservare come questo e altri esempi di servizi che implicano il trattamento di *big data* (corrispondenza elettronica, motori di ricerca) abbiano un legame con il fenomeno *cloud computing* che non può dirsi estraneo alla questione del potere di mercato legato alla concentrazione dei *big data*, posto che i fornitori che controllano infrastrutture *cloud* – solitamente identificati come *over the top* – raccolgono nella «nuvola» grandi (e varie) masse di dati[86]. Al riguardo merita osservare come, in tale contesto, ai rischi di *lock-in* si aggiungano le

---

[83] Cfr. Autorità garante della concorrenza e del mercato, Provvedimento n. 17523, caso n. A375, *Sfruttamento di informazioni commerciali privilegiate*, in *Boll.* n. 40/2007, 95-104; Provvedimento n. 19249, caso n. A375B, *Sfruttamento di informazioni commerciali privilegiate*, in *Boll.* n. 47/2009, 5-20.

[84] Ci si riferisce, in questo caso, all'incompatibilità tecnica tra il formato di rappresentazione dei dati e gli strumenti tecnologici necessari per il loro trattamento.

[85] Sul punto v. Commissione europea, *Sfruttare il potenziale del cloud computing in Europa*, comunicazione del 27 settembre 2012, 6, 11; M. Castellano, F.A. Santangelo, *E-learning e cloud computing*, in G. Fiorentino, (a cura di), *Atti del MoodleMoot Italia 2012*, Livorno, 2012

[86] Cfr. T. Croce, *L'informatica giuridica e le tecnologie della società dell'informazione e della comunicazione*, in *Annali della Facoltà Giuridica dell'Università di Camerino*, n. 2, 2013; C. Flick, V. Ambriola, *Dati nelle nuvole*, *op. cit.*

criticità legate alla possibilità di un'allocazione dei contenuti in *server* decentrati, situati non infrequentemente in zone al di fuori dell'Unione non note agli utenti; condizione, questa, che sul fronte del diritto ripropone la ben nota questione dell'*enforcement* delle regole in internet, e che, per tale motivo, offre il fianco a comportamenti non sempre conformi alle regole unionali. A tal riguardo, i fornitori di *cloud computing* possono effettuare trattamenti all'insaputa di individui e aziende direttamente interessati. In simili casi, sappiamo come gli strumenti giuridici e regolamentari tradizionali, la cui applicazione è geograficamente limitata, non siano sufficienti a limitare le condotte dei detentori dei *big data* che si avvalgono di nuvole che, non infrequentemente, si collocano fuori dalla portata dei predetti strumenti. Il che riporta al più ampio e complesso dibattito sulla regolazione dei comportamenti in internet e sulle ipotesi di *governance* più appropriate, il cui scopo comune dovrebbe essere quello di evitare che la società dell'informazione e della conoscenza possa essere percepita come una prospettiva preoccupante piuttosto che un modello di benessere della collettività.

6. Conclusioni

L'ecosistema digitale è una metafora derivata dalla biologia con cui, da qualche tempo, studiosi e addetti ai lavori sono soliti riferirsi all'ambiente individuato dalle tecnologie dell'informazione e della comunicazione e dalle attività che la comunità svolge al suo interno[87]. La storia di internet ci ricorda, altresì, che l'ambiente compenetrato dalle Ict ha un'origine di "ordine spontaneo", neutrale, e che, a partire dagli anni novanta del secolo passato, questo ordine è stato sottoposto a trasformazioni legate all'ingresso di figure portatrici di interessi diversi e talvolta confliggenti. L'ecosistema digitale viene descritto anche attraverso modelli socioeconomici che, in relazione alle diverse prospettive, esaltano il fattore tecnologico oppure i contenuti trattati con le Ict e i legami con i processi cognitivi o, ancora, i profili di comportamento suscettibili di restringere le libertà fondamentali; al riguardo, sono ben noti i paradigmi della *network society*, della società dell'informazione, della società (e dell'economia) della conoscenza ovvero della società della sorveglianza[88]. Peraltro, al di là delle formalizzazioni utilizzate, va rilevato come

---

[87] Al riguardo, cfr., tra gli altri, Autorità per le garanzie nelle comunicazioni, *La catena del valore e i modelli di business dell'ecosistema digitale*, 2014, reperibile in rete all'indirizzo <http://www.agcom.it/screen-societa-informazione>; Censis, *Condividere la conoscenza per progettare l'innovazione*, Milano, Franco Angeli, 2004, 55 ss.; F. Nachira, *Towardsa network of digital business eco system fostering the local development*, Bruxelles, 2002, reperibile in rete all'indirizzo < www.digital-ecosystems.org/doc/discussionpaper.pdf>.

[88] Sul mutamento della società verso un profilo di rete si veda M. Castells, *La nascita della società in rete*, Milano, Ed. Università Bocconi, 2002. Sulla società dell'informazione si veda A. Mattelart, *Storia della società dell'informazione*, Torino, Einaudi, 2002; D. Lyon, *La società dell'informazione*, Bologna, Il Mulino, 1991. Con riguardo ai modelli della società e dell'economia della conoscenza si possono consultare, tra gli altri, F. Vespasiano, *La società della conoscenza come metafora dello sviluppo*, Milano, Franco Angeli, 2005; D. Foray, *L'economia della conoscenza*, Bologna, Il Mulino, 2006; R. Viale, *Quale mente per l'economia cogni-*

l'impiego delle Ict da parte di famiglie, imprese e settore pubblico abbia determinato la moltiplicazione dei contenuti e, con essa, un processo di evoluzione cognitiva della specie; queste dinamiche hanno segnato una discontinuità rispetto al passato, con l'affermazione del paradigma della conoscenza e, sul fronte economico, con il passaggio dal capitalismo industriale al capitalismo cognitivo[89]. Nel quadro di questi cambiamenti si collocano le fasi che hanno scandito l'evoluzione di internet, in cui, dopo le prime esperienze del *web 1.0*, caratterizzate da un rapporto con gli utenti di tipo statico, privo di interattività (simile al modello verticale della televisione tradizionale), si assiste al passaggio a un formato comunicativo bidirezionale che ha dato origine a iniziative di produzione individuale dei contenuti (*user generated content*) ma anche a pratiche di condivisione degli stessi (*web 2.0*, *web 2.5*). Di queste e altre dinamiche (l'avvento dei motori di ricerca, la nascita dei *social network*, l'*internet of everythings*) va messo in evidenza la capacità di generazione dei contenuti digitali, che è alla base del fenomeno *big data*. L'esperienza della circolazione di queste risorse nella grande Rete ha dato prova del suo stesso carattere virtuoso, favorendo la produzione di nuova conoscenza con la creazione di opere intellettuali (spesso derivate da opere preesistenti, ma dotate di propria autonoma espressione), l'innovazione dei prodotti da parte delle imprese (che si avvalgono delle idee dei consumatori che partecipano ai processi di differenziazione)[90], il progresso scientifico e tecnologico. La centralità, nelle politiche dell'agenda digitale europea, della valorizzazione dei *big data*[91], va dunque collegata all'obiettivo dell'Unione di ridefinire i fondamenti della propria economia nella direzione che già la strategia di Lisbona aveva indicato alla fine del secondo millennio; vale a dire, realizzare un'economia fondata sulla conoscenza[92]. In questa prospettiva, il riutilizzo dei contenuti dei *big data* va considerato anche sotto il profilo cognitivo, ricomprendendo quell'«algoritmo» umano caratterizzato da abilità non codificabili (l'intuizione, la percezione, la creatività, la capacità

tiva, in R. Viale (a cura di) *Le nuove economie*, Milano, Il Sole 24 Ore, 2005. Sulla società della sorveglianza si veda, per tutti, Z. Bauman, D. Lyon, *Sesto potere*, *op. cit.*

[89] La transizione dal capitalismo industriale (orientato alla produzione) al capitalismo cognitivo ha modificato la visione industriale (e fordista) della produzione: la ricchezza prodotta non è attribuita ai processi produttivi tradizionalmente intesi ma è riconducibile all'impiego di risorse individuali di natura biologica, definite dalle funzioni cerebrali dell'uomo. Il fattore lavoro, dunque, si modifica assumendo un profilo immateriale fatto di attività cognitive e comunicative. Sul concetto di capitalismo cognitivo sia consentito un rinvio a G. Crea, *Analisi del comportamento in economia*, Roma, Aracne, 2013, e ai lavori ivi citati. Si veda anche F. Mezzanotte, V. Zeno-Zencovich, *Le reti della conoscenza: dall'economia al diritto*, in *Dir. Inf. Inf.*, n. 2, 2008, 141-171; V. Codeluppi, *Denaro e astrazione sociale nel capitalismo contemporaneo*, in M. Bontempi, V. Cotesta, M. Nocenzi (a cura di), *Simmel e la cultura moderna, Vol. 1: la teoria sociologica di Georg Simmel*, Roma, Morlacchi, 2010, 467-478.

[90] Cfr. Autorità per le garanzie nelle comunicazioni, *Future Internet: scenari di convergenza, fattori abilitanti e nuovi servizi*, reperibile in rete all'indirizzo < http://www.agcom.it/ricerca-screen-offerta-servizi-digitali-e-future-internet>; si veda anche V. Finotto, S. Micelli, *Web e made in Italy: la terra di mezzo della comunicazione d'impresa*, in *Mercati e competitività*, n. 4, 2010, 101-119.

[91] Si veda, al riguardo, Commissione europea, *Verso una florida economia basata sui dati*, 2 luglio 2014, COM(2014) 442.

[92] Si vedano, al riguardo, le Conclusioni del Consiglio europeo di Lisbona, 23-24 marzo 2000.

combinatoria di informazioni e conoscenze)[93] e dunque non traducibili in una sequenza di istruzioni come avviene nel caso di un *software* eseguito da una macchina. Sotto questo aspetto, il riutilizzo si identifica con quel fattore produttivo a cui spesso si riferisce la letteratura sull'economia della conoscenza denominandolo "lavoro cognitivo"[94].Appare allora evidente che se da un lato le Ict possono supportare talune funzioni cognitive, in particolare nei casi in cui, richiamando Simon, la complessità della gestione dei contenuti va oltre le capacità umane (basti pensare alle elaborazioni che devono essere effettuate su dimensioni notevoli di contenuti, e che l'uomo affida ai sistemi informatici), d'altro lato le stesse tecnologie non sostituiscono il lavoro cognitivo; il riutilizzo, cioè, si avvale di tecnologie esterne e "tecnologie interne" tra loro complementari, che dunque si integrano nella produzione della conoscenza. In tale contesto evolutivo restano fermi – e, anzi, assumono maggiore rilevanza – i meccanismi che devono tenere in equilibrio le esigenze di tutela della proprietà intellettuale e dei connessi investimenti con l'interesse alla libera circolazione dei contenuti. Sotto il profilo giuridico, sappiamo che le disposizioni in materia di utilizzazioni libere pongono un limite alle prerogative dei titolari delle opere dell'ingegno per garantire che queste possano essere riutilizzate, anche solo in parte, per scopi di interesse generale (ricerca scientifica, informazione, istruzione) ritenuti prevalenti rispetto a quelli degli autori[95]; a ciò si aggiungano le norme atte a tutelare l'uso delle opere a carattere personale[96]. E così anche il regìme delle licenze *creative commons*, che – diritti morali a parte (es., paternità e integrità dell'opera) – immette l'opera nel pubblico dominio consentendone la rielaborazione funzionale alla produzione di nuovi contenuti[97]. Sul versante del mercato, le limitazioni al diritto di proprietà sulla conoscenza e le buone prassi appaiono idonee a impedire eventuali derive anticoncorrenziali (d'altro

---

[93] In tal senso si veda L. Scognamiglio, *Conoscenza, sviluppo e nuove tecnologie*, Firenze, marzo 2009, reperibile all'indirizzo <http://www.eurosportello.eu/sites/default/files/biblio/Conoscenza-sviluppo-nuove-tecnologie.pdf>.

[94] Si veda, per tutti, E. Rullani, *L'economia della conoscenza nel capitalismo delle reti*, in *Sinergie*, n. 76, 2008, 67-90. L'autore sottolinea come l'utilità (valore) della conoscenza prodotta dal lavoro cognitivo risieda nella moltiplicazione dei suoi impieghi con costi marginali di riproduzione tendenzialmente nulli. Questo valore è superiore a quello del lavoro pre-moderno (artigianale o contadino tradizionale) in cui la conoscenza veniva impiegata per la produzione di uno specifico bene (v. pp. 77-78).

[95] Cfr. G. Cavani, *Le utilizzazioni libere nel campo del diritto d'autore. Esperienze a confronto: la fair use exemption del diritto nordamericano e la disciplina nazionale per casistica*, in *Atti del convegno "Le clausole generali nel diritto commerciale e industriale*, Roma, Università di Roma Tre, 11-12 febbraio 2011. Si veda anche M. Scialdone, *Il nuovo ruolo degli utenti nella generazione di contenuti creativi*, in *Diritto mercato tecnologia*, n. 4, 2013, in cui l'autore, riferendosi al libro verde della Commissione delle comunità europee, *Il diritto d'autore nell'economia della conoscenza*, 2008, alla luce dell'avvento delle Ict, sottolinea la necessità di una riforma dei limiti alle esclusive derivanti dal diritto d'autore per favorire la circolazione delle conoscenze. Al riguardo, vale sottolineare come tra i quesiti posti dalla Commissione agli *stakeholder* sia emerso il tema dell'introduzione nel diritto d'autore di un'eccezione per i contenuti creati dagli utenti.

[96] Cfr. A.M. Gambino, *Creatività e contenuti in rete*, in *Diritto Mercato Tecnologia*, n. 2-3, 2013, 7-18.

[97] Cfr. V. Vinciguerra, *Nota sulle licenze creative commons*, in *Liber Amicorum per Francesco D. Busnelli. Il diritto civile tra principi e regole*, Vol. I, 377 ss.

canto, le ricadute che l'ecosistema digitale ha determinato sui diritti di proprietà, con la riproduzione quasi istantanea della conoscenza, a costi pressoché nulli e senza perdita di qualità, possono essere contrastate ricorrendo a idonei *software* di protezione). Peraltro, anche i meccanismi del mercato hanno dato prova di saper realizzare un equilibrio virtuoso, con l'instaurarsi di relazioni cooperative, tendenzialmente stabili, proprie del mondo delle imprese; al riguardo, la letteratura gius-economica ha evidenziato come tali relazioni siano riconducibili a un modello organizzativo reticolare in cui si privilegia la circolazione delle conoscenze che consente a tutti i membri una costante attività di rielaborazione, condivisione e sfruttamento[98]. Nella sua versione tecnologica, un tale modello si avvale delle reti di telecomunicazioni che, nella prospettiva della condivisione, svolgono la funzione di "moltiplicatori cognitivi".

L'economia della conoscenza resta, pertanto, l'obiettivo strategico europeo nell'orizzonte 2020 a cui vanno ricondotte le politiche volte a garantire il riutilizzo dei contenuti, l'apprendimento continuo (*lifelong learning*), la ricerca, la diffusione della conoscenza; politiche che prospettano un'evoluzione socio-cognitiva, il cui presupposto non può che trovarsi nella circolazione di una moltitudine di contenuti digitali suscettibili di essere riutilizzati. Sotto questo aspetto, le reti di telecomunicazioni rappresentano (insieme al *software*) una risorsa strategica per i paesi detentori, funzionale alla produzione della conoscenza e dunque alla crescita economica e alla loro competitività internazionale. Le tecnologie dell'informazione e della comunicazione individuano pertanto una nuova dimensione della conoscenza in ragione del ruolo di supporto ai processi cognitivi (ossia ai processi sottostanti il lavoro cognitivo) sia sotto il profilo del trattamento dei contenuti sia per gli aspetti relazionali. La dimensione tecnologica della conoscenza si caratterizza per la sua capacità di rimediare ai limiti della razionalità umana, ma anche di opporsi ai sistemi cognitivi «chiusi», propri del paradigma fordista (su cui si è sviluppata la società industriale), per favorire piuttosto la loro apertura a contesti allargati in cui scambiare le risorse cognitive interne con quelle di altri sistemi. La logica *openness*, che ha guidato pensieri e movimenti per l'utilizzo libero di *software* e contenuti, si ripropone, una volta di più, come pratica sociale di condivisione secondo la quale la conoscenza dell'uno fa parte dei processi cognitivi degli altri.

[98] Sul punto, si veda F. Mezzanotte, V. Zeno-Zencovich, *Le reti della conoscenza*, *op. cit.*, 158.

Rivista elettronica di Diritto, Economia, Management

N. 3 - 2015 · pp. 79-86

L'avvento dei droni tra opportunità e problematiche giuridiche

Michele Iaselli

Abstract: L'uso dei droni nell'attuale società civile sta crescendo sempre più negli ultimi tempi e sicuramente la loro introduzione rappresenta una delle innovazioni di maggiore rilevanza. Al di là di impieghi operativi militari, i droni vengono sempre più spesso utilizzati sia per attività di ricognizione (si pensi ad incendi o a calamità naturali particolarmente gravi come terremoti, alluvioni, ecc.) sia per attività collegate a veri e propri servizi (come il trasporto di merci annunciato da Amazon ed anche da Google, oppure si pensi agli usi in campo investigativo o per servizi fotografici o cinematografici). Di recente in Italia la loro regolamentazione è stata affidata all'ENAC con un provvedimento molto discusso in quanto eccessivamente rigido ed articolato. In tale regolamento, però, sono stati solo accennati i maggiori problemi giuridici derivanti da un utilizzo diffuso degli stessi droni ed in particolare si fa riferimento all'inevitabile impatto con la privacy dei cittadini a causa delle diverse tecnologie di cui possono essere dotati (cioè telecamere e microfoni ad alta risoluzione, apparecchiature di imaging termico, dispositivi per intercettare comunicazioni).

The use of drones in the current civil society is growing more and more in recent times and certainly their introduction is one of the innovations of greater importance. Beyond operational use military drones are increasingly being used both for reconnaissance activities (fire or natural disasters particularly serious as earthquakes, floods, etc..) and for activities related to real services (such as the transport of goods from Amazon and also announced by Google, or think of the use in the field or investigative services for photographic or cinematographic). Recently in Italy their regulation has been entrusted with a measure ENAC much discussed as excessively rigid and articulated. In this regulation, however, were only mentioned the major legal issues arising from the widespread use of these drones and in particular refers to the inevitable impact on the privacy of citizens due to the different technologies which can be fitted (cameras microphones and high-resolution thermal imaging equipment, devices for intercepting communications).

Parole chiave: droni, telecamere, privacy, dati personali, RPV, SAPR, consenso, informativa

Sommario: 1. La diffusione dei droni – 2. La regolamentazione ENAC – L'impatto con la privacy e possibili soluzioni – 4. Le responsabilità in caso di incidenti.

Articolo pervenuto il 10 febbraio 2015, approvato il 20 febbraio 2015

1. La diffusione dei droni

Come è noto l'uso dei droni negli ultimi tempi si è particolarmente intensificato ed ormai questi dispositivi vengono impiegati sempre più spesso in attività anche di carattere ludico-commerciale che non hanno niente a che vedere con impieghi operativi militari.
In effetti il drone nasce in ambito militare e può essere definito come un velivolo privo di pilota e comandato a distanza, usato generalmente per operazioni di ricognizione e sorveglianza, oltre che di disturbo e inganno nella guerra elettronica; è indicato nei paesi anglosassoni anche con la sigla RPV, dalle lettere iniziali dell'inglese Remotely Piloted Vehicle «veicolo guidato a distanza».
Nel 2011 gli Stati Uniti, in collaborazione con il Messico, hanno utilizzato i droni per il controllo delle frontiere e per combattere i narcotrafficanti, grazie alla possibilità di monitorarne i movimenti. Nello stesso anno, in Giappone, l'uso dei droni ha permesso di controllare da vicino l'attività dei reattori della centrale nucleare di Fukushima, dopo le esplosioni causate dal terremoto di Tˋ hoku. Per uso bellico, i Predator sono stati impiegati nel 2011 dalle forze statunitensi per proteggere i ribelli in rivolta contro Gheddafi. Proprio un accordo con gli Stati Uniti potrebbe fare dell'Italia il primo Paese, oltre alla Gran Bretagna, ad avere droni statunitensi armati per la protezione delle proprie truppe in Afghanistan: si tratta dei cosiddetti Reaper, più grandi e potenti dei Predator, di cui sei esemplari sono in dotazione dell'Italia. L'intesa potrebbe essere l'inizio di un utilizzo più esteso dei droni armati da parte di molti paesi.
Questi, quindi, sono i principali impieghi di carattere operativo dei droni, ma come si è già avuto modo di sottolineare anche l'ambito civile ormai sta vedendo un uso sempre più generalizzato di droni sia per attività di ricognizione (si pensi ad incendi o a calamità naturali particolarmente gravi come terremoti, alluvioni, ecc.) sia per attività collegate a veri e propri servizi (come il trasporto di merci annunciato da Amazon ed anche da Google, oppure si pensi agli usi in campo investigativo o per servizi fotografici o cinematografici).

2. La regolamentazione ENAC

Già da tempo, quindi, era nata la necessità di regolamentare l'uso di questi dispositivi e solo il 16 dicembre del 2013 l'ENAC con uno specifico regolamento ha deciso di intervenire in modo piuttosto rigoroso dettando delle regole particolarmente incisive che sono entrate in vigore il 30 aprile del 2014 creando non pochi problemi applicativi.
In particolare il regolamento usa innanzitutto un linguaggio più rigoroso parlando di mezzi aerei a pilotaggio remoto da inquadrare nella categoria degli aeromobili disciplinati dall'art. 743 del codice della navigazione.
Il regolamento distingue, inoltre, ai fini dell'applicazione delle disposizioni del Codice della navigazione, i mezzi aerei a pilotaggio remoto in Sistemi Aeromobili a Pilotaggio Remoto e Aeromodelli.

I mezzi aerei a pilotaggio remoto impiegati o destinati all'impiego in operazioni specializzate o in attività sperimentali, costituiscono i Sistemi Aeromobili a Pilotaggio Remoto (SAPR) e ad essi si applicano le previsioni del Codice della Navigazione secondo quanto previsto dal Regolamento.
Gli aeromodelli, invece, non sono considerati aeromobili ai fini del loro assoggettamento alle previsioni del Codice della Navigazione e possono essere utilizzati esclusivamente per impiego ricreazionale e sportivo.
Ai fini della concreta applicabilità il regolamento chiarisce di poter disciplinare solo i SAPR di massa massima al decollo non superiore a 150 kg e tutti quelli progettati o modificati per scopi di ricerca, sperimentazione o scientifici oltre ovviamente agli aeromodelli.
In particolare per una migliore e più articolata disciplina il regolamento distingue tra SAPR con mezzi aerei di massa massima al decollo minore di 25 kg e SAPR con mezzi aerei di massa massima al decollo uguale o maggiore di 25 kg.[1]
Avuto riferimento ai primi il regolamento[2] prevede che l'impiego dei SAPR è soggetto al possesso di appropriate autorizzazioni rilasciate dall'ENAC all'operatore o alla presentazione da parte dell'operatore di una specifica dichiarazione all'ENAC. In altri termini la capacità dell'operatore del SAPR a rispettare gli obblighi derivanti dal Regolamento viene attestata dall'ENAC mediante una autorizzazione nei casi di operazioni di volo critiche, mentre nei casi di operazioni di volo non critiche, tale capacità viene dichiarata dall'operatore secondo le modalità previste nel Regolamento.
Per operazioni specializzate non critiche si intendono quelle operazioni che non prevedono il sorvolo, anche in caso di avarie e malfunzionamenti, di:

1. aree congestionate, assembramenti di persone, agglomerati urbani e infrastrutture;
2. aree riservate ai fini della sicurezza dello Stato;
3. linee e stazioni ferroviarie, autostrade e impianti industriali.

Tali operazioni sono condotte nel volume di spazio di 70 m di altezza massima dal terreno e di raggio di 200 m. (V70) e nell'ambito delle seguenti condizioni:

- ad una distanza orizzontale di sicurezza adeguata dalle aree congestionate, ma non inferiore a 150 m, e ad una distanza di almeno 50 m da persone e cose, che non siano sotto il diretto controllo dell'operatore;
- in condizioni di luce diurna;
- in spazi aerei non controllati;
- fuori dalle ATZ[3] e comunque ad almeno 8 km dal perimetro di un aeroporto e dai sentieri di avvicinamento/decollo di/da un aeroporto.

Per operazioni specializzate critiche, si intendono, invece, quelle operazioni svolte in condizioni nelle quali il pilota remoto rimane in contatto visivo con il mezzo aereo (VLOS)[4]

---

[1] Art. 7 Regolamento ENAC

[2] Art. 8 Regolamento ENAC

[3] Aerodrome Traffic Zone

[4] Visual Line of Sight

nell'ambito di limitazioni/condizioni che non rispettano, anche solo parzialmente, le situazioni precedenti.
Situazione ben diversa è per i Sistemi Aeromobili a Pilotaggio Remoto con mezzi aerei di massa massima al decollo maggiore o uguale a 25 kg, difatti essi devono essere registrati dall'ENAC mediante iscrizione nel Registro degli Aeromobili a Pilotaggio Remoto, con l'apposizione di marche di registrazione dedicate.[5]
L'abilitazione alla navigazione è attestata dal rilascio di un Permesso di Volo al SAPR, o da un Certificato di Navigabilità Ristretto nel caso di SAPR in possesso di un Certificato di Tipo Ristretto che attesta la rispondenza alla base di certificazione stabilita dall'ENAC, determinata tenendo conto delle specificità del sistema e delle sue modalità di impiego.[6]
Il Permesso di Volo può essere rilasciato in due casi:
a. per effettuare la sperimentazione allo scopo di ricerca e sviluppo o di dimostrazione di rispondenza alla base di certificazione nel caso di SAPR per i quali è stato richiesto un certificato di tipo ristretto;
b. per operazioni specializzate nel caso di SAPR non costruiti in serie e quindi non in possesso di certificazione di tipo ristretto.
Il Permesso di volo viene rilasciato a seguito di operazioni di verifica sulla documentazione presentata e nel caso di operazioni specializzate è rilasciato al termine, con esito positivo, degli accertamenti necessari a verificare che le operazioni previste possono essere condotte con un livello di sicurezza adeguato.
Il certificato di navigabilità ristretto, invece, viene rilasciato al singolo SAPR a seguito di presentazione da parte del proprietario di una dichiarazione del costruttore che attesta che il SAPR è conforme al tipo certificato.
Naturalmente per eseguire operazioni specializzate anche l'operatore del SAPR deve essere autorizzato dall'ENAC dimostrando di possedere tutta una serie di requisiti tecnici e formali.
Purtroppo non finiscono qui le formalità richieste per utilizzare i droni che rientrando nella categoria degli aeromobili sono naturalmente sottoposti a formalità ed accertamenti molto rigorosi. Di conseguenza è necessario essere ammessi allo spazio aereo nazionale rispettando le regole dell'aria[7] nonché tutti gli altri Regolamenti emanati dall'ENAC ed applicabili agli spazi aerei. Inoltre il pilota del SAPR oltre a dimostrare la conoscenza delle predette regole e possedere la necessaria idoneità psico-fisica, deve aver effettuato un programma di addestramento per lo specifico SAPR.[8]
Naturalmente i SAPR devono essere equipaggiati con i dispositivi/sistemi necessari per l'effettuazione delle operazioni previste in accordo alle regole dell'aria applicabili e in funzione degli spazi aerei impegnati, inclusi equipaggiamenti che permettano al pilota di

[5] Art. 9 Regolamento ENAC

[6] Art. 10 Regolamento ENAC

[7] Art. 16 Regolamento ENAC

[8] Art. 17 Regolamento ENAC

comunicare con l'Ente di controllo del traffico aereo.[9]
Regole meno severe sono ovviamente dettate per gli aeromodelli. In particolare, viene chiarito che l'aeromodellista ai comandi dell'aeromodello ha la responsabilità di utilizzare il mezzo in modo che non possa arrecare rischi a persone o beni a terra e ad altri utilizzatori dello spazio aereo, inoltre è tenuto a mantenere la separazione da ostacoli, evitare collisioni in volo e dare precedenza a tutti.[10]
L'aeromodellista è anche responsabile di ottemperare agli obblighi relativi e deve ottenere le eventuali autorizzazioni per l'utilizzo dello spettro elettromagnetico impegnato dal radiocomando.
Anche nel caso degli aeromodelli viene fatta una distinzione fra quelli con massa al decollo massima minore di 25 kg e quelli con massa al decollo massima uguale o maggiore a 25 kg prevedendo per questi ultimi regole più rigide quali la maggiore età richiesta all'aeromodellista.

3. L'impatto con la privacy e possibili soluzioni

Ma il vero problema rappresentato dall'utilizzo di questi droni è sicuramente quello del rispetto della privacy e della protezione dei dati. Difatti le particolari caratteristiche di questi dispositivi che sono in grado di effettuare foto, registrare audio e immagini impone una maggiore attenzione e regolamentazione per la tutela della collettività sul fronte del trattamento dei dati. In merito a questo aspetto il Regolamento dell'ENAC è naturalmente deficitario in quanto all'art. 23 si limita ad operare un rinvio ai principi del Codice in materia di protezione dei dati personali, in particolare al principio di necessità di cui all'art. 3, ed a eventuali provvedimenti dell'Autorità Garante che effettivamente già ha lasciato intendere di dover quanto prima regolamentare questo delicato settore.
Naturalmente il rischio è quello di imbrigliare questi dispositivi nell'ambito di una fitta rete di regole da rispettare (come ha già fatto l'ENAC dal punto di vista tecnico) rendendone di fatto difficile l'utilizzazione. Come è noto i droni sono estremamente utili nel settore pubblico per raccogliere notizie ed informazioni avuto riferimento a gravi situazioni di emergenza come incendi boschivi ed inondazioni ed almeno in questi casi sarebbe opportuno prevedere una maggiore elasticità. Riguardo, invece, i più recenti utilizzi di natura privatistica degli stessi droni, cui si è già accennato all'inizio di questo lavoro, effettivamente sarebbe opportuna una più attenta regolamentazione che impedisca prevedibili violazioni della privacy. Il quadro generale diventa più preoccupante se si pensa alla recente invasione sul mercato di questi dispositivi acquistabili, nelle versioni base, per poche centinaia di euro. Potranno anche essere considerati alla stessa stregua di aeromodelli, ma rimangono comunque "pericolosi" per le loro intrinseche caratteristiche.Anche gli Stati Uniti stanno pensando all'emanazione di linee guida sulla privacy per l'uso commerciale di droni.

[9] Art. 18 Regolamento ENAC

[10] Art. 23 Regolamento ENAC

In ambito europeo il gruppo art. 29[11] ha manifestato una certa preoccupazione in materia riconoscendo la necessità di concentrarsi sulle minacce che una proliferazione incontrollata di droni potrebbero portare ai diritti ed alle libertà fondamentali delle persone.
Naturalmente dal punto di vista della protezione dei dati, ciò che è rilevante non è tanto l'uso dei droni come tali, ma lo sono le diverse tecnologie di cui possono essere dotati (cioè telecamere e microfoni ad alta risoluzione, apparecchiature di imaging termico, dispositivi per intercettare comunicazioni) e la successiva raccolta e il trattamento dei dati personali che si configurerebbe, talvolta nei confronti di persone ignare in considerazione delle limitate dimensioni di alcuni di questi dispositivi in grado di operare in volo. Inoltre qualora gli stessi droni fossero visibili, sarebbe estremamente difficile, se non impossibile, sapere chi ci sta osservando, per quali finalità e come esercitare i relativi diritti.
Da un punto di vista normativo, le prime regolamentazioni di carattere internazionale in materia, hanno considerato applicabili le disposizioni generali sulla videosorveglianza al trattamento dei dati personali connessi all'uso di droni insieme alle norme generali sulla protezione dei dati, quali la notifica e il diritto degli interessati di essere informati.
Riguardo un possibile futuro quadro normativo, nessuno dei provvedimenti attualmente in discussione a livello comunitario (regolamento generale sulla protezione dei dati e regolamento in materia di polizia e giustizia, direttiva sulla protezione dei dati in materia penale) comprendono disposizioni specifiche relative al trattamento dei dati personali effettuato per mezzo di droni.
Di conseguenza appare plausibile che, come già accade ogni qualvolta ci si trovi di fronte a nuovi disposizioni tecnologiche, siano innanzitutto applicabili le disposizioni generali in materia di protezione dei dati personali a tale trattamento.
Le nuove disposizioni in materia di valutazione d'impatto sulla protezione dei dati, i principi della privacy by design e by default e le disposizioni specifiche in materia di certificazione delle operazioni di trattamento dei dati possono essere di particolare rilevanza per disciplinare la protezione dei dati e le minacce legate all'utilizzo dei droni.
Il progetto di regolamento europeo in materia di protezione dei dati[12] introduce l'obbligo per i responsabili di effettuare una valutazione d'impatto sulla protezione dei dati prima di effettuare operazioni di trattamento a rischio, come il monitoraggio delle aree accessibili al pubblico, in particolare quando i dispositivi ottici-elettronici (videosorveglianza) sono utilizzato su larga scala.
Ai sensi dell'articolo 23, paragrafo 2, del progetto di regolamento, il responsabile del trattamento deve adottare meccanismi per garantire che, per impostazione predefinita, vengano trattati solo i dati personali necessari per ciascuna finalità specifica del trattamento e che i dati siano soprattutto non raccolti o conservati al di là del minimo necessario.
Il principio della privacy by design prevede che la protezione dei dati sia integrata nell'intero ciclo di vita della tecnologia, dalla primissima fase di progettazione fino alla sua ultima distribuzione, all'utilizzo e all'eliminazione finale.

---

[11] Remotely Piloted Aircraft Systems (RPAS) – Response to the Questionnaire – 16/12/2013

[12] Art. 33 schema di Regolamento Europeo in materia di protezione dei dati

Il principio della privacy by default prevede che le impostazioni di tutela della vita privata relative ai servizi e prodotti rispettino i principi generali della protezione dei dati, quali la minimizzazione dei dati e la limitazione delle finalità.
La privacy by design può essere definita la nuova dimensione della privacy che trae le sue origini dall'innovazione tecnologica e dal progresso delle comunicazioni elettroniche.
L'evoluzione, quindi, tocca anche il settore della privacy rispetto alla tradizionale e primaria configurazione con il riferimento alle PET (acronimo di Privacy Enhancing Technologies) che costituiscono le tecnologie utilizzate per migliorare il diritto alla privacy. Ovviamente tali tecnologie vengono considerate in maniera neutra, ovvero senza alcuna connessione con specifiche fattispecie.[13]
Il concetto di Privacy by Design trova spazio nella trilogia di applicazioni: 1) IT systems; 2) accountable business practices; and 3) physical design and infrastructure". In sostanza:
1) Tecnologia dell'informazione;
2) Pratiche commerciali responsabili;
3) Progettazione delle strutture.
Il rischio di sorveglianza generalizzata derivanti dall'uso dei droni richiede specifiche disposizioni al fine di evitare l'uso improprio di queste tecnologie e ridurre al minimo le interferenze con i diritti e le libertà fondamentali in conformità con i principi generali di protezione ben noti.
Naturalmente come già è accaduto nel Regolamento dell'ENAC, il quadro giuridico che verrà adottato per garantire l'integrazione graduale di sicurezza dei droni nel sistema europeo di gestione del traffico aereo (ATM) dovrebbe chiaramente fare riferimento alla necessità di rispettare la legislazione sulla protezione dei dati.
Il coinvolgimento delle Autorità dell'aviazione civile competenti nella verifica dell'adempimento degli obblighi di protezione dei dati da parte dei responsabili dei dati, prima di concedere loro l'autorizzazione richiesta, potrebbe essere fondamentale ai fini di un'efficace tutela della privacy in questo delicato settore.

4. Le responsabilità in caso di incidenti

Tra le disposizioni più criticate del Regolamento vi è sicuramente l'art. 20 che prevede la necessità di stipulare un'assicurazione concernente la responsabilità verso terzi, adeguata allo scopo e non inferiore ai massimali minimi previsti dalla normativa europea. Tale disposizione nasce dalla consapevolezza di possibili incidenti che potrebbero verificarsi nonostante le prescrizioni molto severe del Regolamento.
Si fa in particolare riferimento alla tabella di cui all'art. 7 del Regolamento (CE) n. 785/2004 che richiede ai vettori aerei e agli esercenti di aeromobili un'assicurazione per la respon-

[13] Tale espressione fu utilizzata per la prima volta nel report pubblicato nel 1995 dal titolo "Privacy-enhancing technologies: the path to anonymty", della Data Protection Authority olandese in collaborazione con il Commissario dell'Ontario (Canada).

sabilità civile verso i terzi con massimali minimi variabili, per ciascun aeromobile e per incidente (rischi ordinari e c.d. rischi guerra), a seconda del MTOM (peso massimo al decollo).
L'obbligo assicurativo non opera invece per gli aeromodelli.
In altri termini, quindi, il drone, viene equiparato ad un'autovettura anche se all'attualità il suo uso presenta molti più rischi, se non altro per la particolare tecnologia che lo contraddistingue che fa avvicinare il drone ad un vero e proprio sistema cognitivo artificiale.
Lo stesso aeromodello, se vogliamo, presenta molti rischi probabilmente sottovalutati a livello normativo, vista la non obbligatorietà dell'assicurazione.
Ma a questo punto in caso di incidente di chi è la responsabilità? Del produttore, dell'operatore o del pilota?
Diverse difatti sono le figure che contraddistinguono il mondo dei droni:
- Il produttore che è colui che costruisce e commercializza (in realtà le due figure potrebbero anche essere diverse) il drone;
- L'operatore che è colui che gestisce e manutenziona il drone;
- Il pilota che è colui che viene incaricato dall'operatore responsabile della condotta del volo ed agisce sui comandi di volo.

Inoltre va tenuto presente che in caso di operazioni specializzate per conto terzi, deve essere stipulato un accordo tra l'operatore del drone e il committente nel quale le parti definiscono le rispettive responsabilità e concordano sull'idoneità del drone per la specifica operazione di volo e sulle eventuali limitazioni e condizioni connesse.
A ben guardare, quindi, il problema della responsabilità non è affatto facile da risolvere ed è fondamentale a questo punto analizzare con attenzione la meccanica dell'incidente al fine di valutare tutte le variabili che sono fondamentali ai fini dell'imputazione della relativa responsabilità. Indubbiamente appare evidente che più il drone viene automatizzato più le relative responsabilità si spostano a carico del produttore, in quanto il margine di errore del pilota viene sempre più ridotto e lo stesso operatore finisce per avere sempre meno obblighi di manutenzione.

N. 3 - 2015 · pp. 87-96

La data retention dopo la dichiarazione di invalidità della Direttiva 2006/24/CE

Giulio Pascali

Abstract: Con sentenza dell'8 aprile 2014, la Corte di Giustizia dell'Unione Europea ha sancito la invalidità della Direttiva 2006/24/CE, che aveva modificato la Direttiva 2002/58/CE, introducendo nel sistema normativo europeo alcune fondamentali indicazioni sulla conservazione dei dati personali nell'ambito dei servizi di comunicazione elettronica. Nell'attesa che intervenga una nuova disciplina, è opportuno esaminare quali effetti possa sortire la pronuncia comunitaria, e quali strade possa prendere la disciplina nazionale ed europea, partendo dalle indicazioni della Corte.

Abstract: With a decision dated April 8th, 2014, the Court of Justice of the European Union has voided Directive EC/2006/24, which amended Directive EC/2002/58 and introduced the discipline on data retention in the electronic communications field. Until new regulation on the matter is issued by the European Community, this document seeks to examine the effects of the decision of the EUCJ, and the path both national and european regulation might take in the meantime, following the principles sanctioned with the pronunciation thereof.

Parole chiave: privacy, protezione dei diritti fondamentali, CGUE, Corte di Giustizia UE, Europa, diritti fondamentali, servizi di comunicazione elettronica, *data retention*, telecomunicazioni

1. Introduzione e quadro normativo di riferimento

Nel novero dei diritti fondamentali dell'individuo, a partire dalla iniziale elaborazione dottrinaria e giurisprudenziale Americana[1], ha assunto sempre maggiore importanza il

[1] Furono i giuristi Samuel Warren e Louis Brandeis, in un noto articolo pubblicato il 15 dicembre 1890 sull'*Harvard Law Review*, a definire per la prima volta il Diritto alla Privacy come "uno dei più importanti diritti dell'individuo" (S.D. Warren – L.D. Brandeis "*The Right to Privacy*", Harvard Law Review, Vol. IV, No. 5, Boston, 1890)

Articolo pervenuto il 10 febbraio 2015, approvato il 20 febbraio 2015

diritto alla Privacy. Il concetto stesso di Privacy ha subito nel tempo notevoli evoluzioni, passando da un mero "diritto ad essere lasciati in pace"[2] ad un complesso agglomerato di situazioni e prescrizioni, frutto di un continuo quanto vario bilanciamento dei diritti che ad esso si rapportano e si confrontano.

La complessità di tale diritto rende certamente altrettanto complessa la predisposizione di strumenti di tutela, con la naturale conseguenza per la quale spesso il legislatore, le autorità indipendenti e gli stessi singoli individui interessati debbano compiere una valutazione strettamente *case-by-case* in merito all'applicabilità dei principi fondamentali in materia al caso concreto in analisi.

Con l'avvento dell'Unione Europea, la Privacy è stata definita quale diritto fondamentale, approdando quindi ad una codificazione nella Carta dei Diritti Fondamentali dell'Unione Europea[3], il cui art. 8 specificamente afferma il diritto di ogni individuo alla protezione dei dati di carattere personale che lo riguardano, secondo specifici principi fondamentali[4].

Prima ancora della Carta di Nizza, tuttavia, la Privacy dell'individuo era già stata oggetto di molteplici interventi normativi comunitari, con una serie di Direttive che avevano definito il quadro generale del contenuto di tale diritto e degli strumenti per la tutela dello stesso[5].

Al quadro generale, già complesso nella sua pluriennale articolazione, il legislatore comunitario ha inoltre aggiunto specifiche disposizioni per la tutela della Privacy in uno specifico settore, quello delle c.d. "comunicazioni elettroniche". La più recente elaborazione normativa comunitaria in materia è rappresentata da due Direttive, oggetto della sentenza in commento, che hanno sostanzialmente codificato in ambito comunitario e nei singoli stati membri i principi fondamentali e le tutele di base, solitamente demandando ai legislatori nazionali l'articolazione di tali principi e tutele nelle forme più adeguate[6].

La prima Direttiva, n. 2002/58/CE[7], parte del c.d. "Pacchetto Telecom" unitamente

---

[2] Warren e Brandeis muovono nel citato saggio dai concetti di diffamazione, reputazione e di diritto alla protezione della proprietà intellettuale, per approdare, infine, ad un testuale "*right to be let alone*", proprio di tutti gli individui membri della società civile.

[3] La c.d. "Carta di Nizza", provv. 2000/C 364/01 del 18 dicembre 2000.

[4] L'articolo 8 della Carta di Nizza, infatti, testualmente recita:
"*1. Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano.*
2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica.
3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente"

[5] Prima fra tutte la Direttiva 95/46/CE del 24 ottobre 1995 "*relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati*"

[6] Sulla Privacy in Rete, si veda E. Falletti "*L'evoluzione del concetto di Privacy e della sua tutela giuridica*" in G. Cassano – G. Scorza – G. Vaciago "*Diritto dell'Internet*", CEDAM 2013, p. 21 e ss.

[7] Che già riformava e sostituiva la previgente Direttiva 97/66/CE del 15 dicembre 1997 "*sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni*"

alle direttive c.d. "*Quadro Generale*"[8], "*Sull'Accesso e sull'Interconnessione*"[9], "*Sulle autorizzazioni e le licenze*"[10] e "*Sul Servizio Universale*"[11], pone le basi fondamentali per l'armonizzazione del diritto interno degli Stati Membri dell'Unione Europea, relativamente alla tutela del diritto alla vita privata, con special riguardo al trattamento dei dati personali nel settore delle comunicazioni, con l'obiettivo di assicurare al tempo stesso la libera circolazione dei dati, delle apparecchiature e dei servizi di comunicazione elettronica all'interno dell'Unione. Integrando, dunque, quanto già previsto dalla Direttiva 95/46/CE in materia di trattamento dei dati personali, la Direttiva 2002/58/CE fornisce una aggiornata definizione di concetti come la riservatezza delle comunicazioni effettuate tramite la rete pubblica di comunicazione e i servizi di comunicazione elettronica accessibili al pubblico, l'automatica cancellazione e/o anonimizzazione dei dati di traffico degli abbonati/utenti, trattati nell'ambito di un servizio di comunicazione elettronica, e, ancora, regola il trattamento dei dati relativi all'ubicazione diversi dai dati di traffico. In linea generale, la Direttiva fissa generali divieti di trattamento e/o limiti temporali per la conservazione dei dati acquisiti, introducendo infine talune specifiche deroghe, basate sul principio della temporaneità e del contemperamento della riduzione delle tutele in rapporto ai diritti fondamentali dell'utente coinvolti[12].
La seconda Direttiva, n. 2006/24/CE, approfondisce taluni aspetti della privacy nel peculiare settore delle comunicazioni elettroniche, mediando tra le esigenze di prevenzione e repressione dei reati e la privacy dei singoli individui.

2. Il contenuto della Direttiva 2006/24/CE

Nata dalla crescente necessità di regolamentare aspetti del diritto alla Privacy originariamente non contemplati nella normativa comunitaria, ed emersi in stretto rapporto con l'evoluzione tecnologica, la Direttiva 2006/24/CE riguarda "*la conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione*", ed espressamente modifica la previgente Direttiva 2002/58/CE, aggiornandone taluni specifici contenuti.

---

[8] Direttiva 2002/21/CE del Parlamento Europeo e del Consiglio, adottata il 7 marzo 2002, che "*istituisce un quadro normativo comune per le reti ed i servizi di comunicazione elettronica*".

[9] Direttiva 2002/19/CE del Parlamento Europeo e del Consiglio, adottata il 7 marzo 2002, relativa all'accesso alle reti di comunicazione elettronica e alle risorse correlate, e all'interconnessione delle medesime.

[10] Direttiva 2002/20/CE del Parlamento Europeo e del Consiglio, adottata il 7 marzo 2002, relativa alle autorizzazioni per le reti e i servizi di comunicazione elettronica.

[11] Direttiva 2002/22/CE del Parlamento Europeo e del Consiglio, adottata i 12 luglio 2012, relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica.

[12] Per chiarire meglio il concetto, è proprio nella Direttiva in parola che è stata prevista, tra le varie, la possibilità di annullare in via temporanea la soppressione dell'identificativo di linea chiamante richiesto, su specifica richiesta di un abbonato, per i soli fini di identificare e perseguire autori di chiamate malintenzionate e/o importune (art. 10, comma 1, lett. a)).

Ad una iniziale analisi strutturale, la Direttiva si rivela sin da subito come introduttiva di deroghe alle ordinarie misure di protezione dei dati personali di cui agli artt. 5, 6 e 9 della Direttiva 2002/58/CE, in ragione degli specifici strumenti tecnologici adottati per il trattamento dei dati in questione[13].

Il legislatore comunitario, preso atto che le comunicazioni telefoniche e telematiche avrebbero assunto un ruolo sempre maggiore non solo per lo sviluppo della Società civile, ma anche per quello dei fenomeni di illegalità ad essa sottesi, individua alcune categorie di c.d. "dati" di traffico (ma non solo) che, opportunamente conservati dai fornitori stessi dei servizi di comunicazione elettronica, possono essere richiesti ed utilizzati dalle competenti Autorità ai fini dell'accertamento e prevenzione dei reati gravi. Pur nella sua ormai datata configurazione definitoria, la Direttiva individua le seguenti tipologie di dati da conservare:

a) dati per rintracciare e identificare la fonte di una comunicazione (art. 5, comma 1, lett. a));
b) dati necessari per rintracciare e identificare la destinazione di una comunicazione (art. 5, comma 1, lett. b));
c) dati necessari per determinare la data, l'ora e la durata di una comunicazione (art. 5, comma 1, lett. c));
d) dati necessari per determinare il tipo di comunicazione (art. 5, comma 1, lett. d));
e) dati necessari per determinare le attrezzature di comunicazione degli utenti o quello che si presume essere le loro attrezzature (art. 5, comma 1, lett. e));
f) dati necessari per determinare l'ubicazione delle apparecchiature di comunicazione mobile (art. 5, comma 1, lett. f) .

Come è agevole notare, nessuna delle categorie sopra censite riguarda il contenuto delle comunicazioni, la cui conservazione è anzi espressamente vietata dalla Direttiva[14].

Non sfugge tuttavia anche al lettore non avvezzo al linguaggio giuridico, come l'insieme di una o più categorie di dati sopra elencate possa comunque operare uno o più suggestivi rimandi al contenuto delle comunicazioni, pur non riportandolo *de plano*.

La Direttiva individua un periodo di tempo minimo e massimo per la conservazione dei dati sopra elencati: ai sensi dell'art. 6, infatti, "*gli Stati Membri provvedono affinché le categorie di dati […] siano conservate per periodi non inferiori a sei mesi e non superiori a due anni dalla data della comunicazione*".

Anche per quanto riguarda la protezione e la sicurezza dei dati trattati, la Direttiva fissa

---

[13] Il Considerando n.3 recita infatti: "*Gli articoli 5, 6 e 9 della direttiva 2002/58/CE definiscono le norme applicabili al trattamento, da parte dei fornitori di reti e servizi, dei dati relativi al traffico e dei dati relativi all'ubicazione generati dall'uso di servizi di comunicazione elettronica. Questi dati devono essere cancellati o resi anonimi quando non sono più necessari ai fini della trasmissione di una comunicazione, tranne per quanto riguarda i dati necessari per la fatturazione o per il pagamento dell'interconnessione […]*"

[14] Lo stesso comma 2 dell'art.5 della Direttiva prescrive che "*a norma della presente direttiva, non può essere conservato alcun dato relativo al contenuto della comunicazione*".

alcuni principi di base, lasciando poi ai singoli Stati Membri l'adozione di normativa di dettaglio[15][16].

3. I rilievi della Corte di Giustizia

All'esame della Corte di Giustizia UE sono stati proposti due differenti casi, riuniti per affinità, in cui giudici nazionali (rispettivamente membri di corti giudiziarie in Irlanda ed Austria) hanno ritenuto necessario richiedere opportuni chiarimenti sulla interpretazione normativa della Direttiva 2006/24/CE, nonché sulla compatibilità della Direttiva in questione con i princìpi di diritto dei Trattati istitutivi dell'Unione Europea e della Carta Europea dei Diritti Fondamentali.
In entrambi i casi, i giudici nazionali avevano ritenuto di operare il rinvio interpretativo alla CGUE in merito al rispetto, da parte della Direttiva 2006/24/CE, della Carta dei Diritti dell'Unione Europea, articoli 7 e 8[17].
In primo luogo, la Corte ha esaminato le ragioni sottese all'adozione della Direttiva contestata, concludendo per la sostanziale correttezza delle stesse: nell'opinione del giudice comunitario, il rispetto dei diritti fondamentali può essere temperato e modulato in ragione delle generali esigenze di tutela nazionale ed internazionale per la repressione

---

[15] In Italia, ad esempio, il d.lgs. n.196/2003 "*Codice in materia di Protezione dei Dati Personali*", ha recepito le indicazioni della Direttiva agli articoli 123 e ss.
In particolare, la normativa Italiana prevede il seguente regime, per i dati di traffico telefonico e/o telematico:
- la generale previsione della cancellazione e/o anonimizzazione "*quando non sono più necessari ai fini della trasmissione della comunicazione elettronica*", fatti salvi i casi disciplinati (art. 123, c.1);
- l'ulteriore generale previsione di esclusione dalla conservazione dei contenuti delle comunicazioni (art. 132, c.1);
- la possibilità di conservare i dati strettamente necessari a fini di fatturazione, o a pagamenti in caso di interconnessione, "*per un periodo non superiore a sei mesi, salva l'ulteriore specifica conservazione necessaria per effetto di una contestazione anche in sede giudiziale*" (art. 123, c.2);
- la possibilità di conservare i dati di traffico telefonico "*per ventiquattro mesi dalla data della comunicazione*" e di conservare i dati di traffico telematico "*per dodici mesi dalla data della comunicazione*", in entrambi i casi "*per finalità di accertamento e repressione dei reati*" (art. 132, c.1).

A tale regime vengono affiancati l'obbligatorio transito dei dati dal database semestrale a quello annuale/biannuale alle relative scadenze di legge, nonché un rigoroso elenco dei soggetti autorizzati a richiedere tali informazioni.

[16] Per un primo commento critico al D.lgs. n.109 del 30 maggio 2008, che ha attuato la Direttiva 2006/24/CE, si veda S. Aterno – A. Cisterna "*Il legislatore interviene ancora sul data retention, ma non è finita*", in Diritto Penale e processo, n.3/2009, p.279 e ss.

[17] Il dettaglio delle vicende processuali dalle quali promana la sentenza in commento, unitamente ad una disamina dei precedenti giurisprudenziali nazionali ed internazionali della stessa può essere reperita nei commenti di C.M. Cascione "*I diritti fondamentali prevalgono sull'interesse alla sicurezza: la decisione data retention della corte di giustizia e gli echi del datagate*", in *Nuova Giurisprudenza Civile commentata*, n.11/2014, p. 1039 e ss., e L. Trucco "*Data retention: la Corte di giustizia si appella alla Carta UE dei diritti fondamentali*", in *Giurisprudenza Italiana*, n.8-9/2014, p.1850 e ss.

dei reati. *Nulla quaestio*, dunque, sui motivi dell'intervento normativo.
Ciò che tuttavia la Corte contesta riguarda, più specificamente, la *proporzionalità* dell'intervento operato dal legislatore comunitario, in rapporto ai diritti fondamentali degli individui che risiedono nel territorio dell'Unione:

- in primo luogo, argomenta la Corte, se la Direttiva mira a contribuire alla lotta alla criminalità grave, è pur vero che la stessa non limita la conservazione dei dati nel tempo e/o in una specifica area geografica e/o ad una cerchia di persone determinate che possano essere coinvolte nell'ipotesi di reato;
- altra grave mancanza della Direttiva è costituita dalla sostanziale assenza di limitazione oggettiva dei reati che permettono l'accesso delle Autorità competenti ai dati di traffico dei singoli soggetti. Non basta, per la Corte, insomma, il mero "rinvio" alle normative degli Stati Membri, per definire quali reati debbano essere considerati "gravi" e quali no; meglio sarebbe stato se il legislatore comunitario avesse effettivamente individuato le fattispecie di reato che, per la loro particolare lesività e gravità, giustificassero l'accesso delle Autorità ai dati di traffico[18];
- la Direttiva omette, inoltre, di specificare le condizioni sostanziali e procedurali relative all'accesso ai dati, da parte delle Autorità competenti. Anche in questo caso, per la Corte non è sufficiente il rinvio alla normativa dei singoli Stati Membri, per assicurare il rispetto dei principi fondamentali di cui alla Carta UE;
- altra grave omissione prescrittiva, secondo la Corte, è rappresentata dall'assenza di limiti all'accesso ai dati di traffico: stando, in effetti, al dettato della sola Direttiva, non sarebbe nemmeno necessaria una valutazione giudiziale, per poter accedere a tali dati, e manca persino, in tal senso, un obbligo per gli Stati Membri di prevederla;
- ancora, per ciò che riguarda la conservazione dei dati, la Direttiva impone un termine generico di "*almeno 6 mesi*", senza effettuare alcuna distinzione tra le varie categorie di dati, pur definiti nella Direttiva stessa. Una tale generalizzazione, secondo la Corte, compromette seriamente la legittimità della prescrizione normativa;
- sempre per quanto attiene la conservazione dei dati acquisiti, la Direttiva stabilisce tempistiche la cui durata di colloca tra un minimo di 6 mesi ed un massimo di 24 mesi, senza tuttavia individuare precisi criteri per la determinazione del periodo, in relazione al generale obbligo di trattamento dei dati acquisiti "*per il tempo stretto necessario*";
- proseguendo nella disamina delle carenze della Direttiva, la Corte individua anche la generale assenza di specifiche garanzie per la sicurezza e la protezione dei dati personali (anche da abusi che potrebbero essere posti in essere dalle Autorità nel corso di legittimi

[18] La Commissione Europea non ha mai fatto mistero che le disposizioni contenute nella Direttiva sulla *Data Retention* fossero state adottate nel delicato periodo successivo agli attentati di Madrid e Londra (si veda sul punto http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/police-cooperation/data-retention/index_en.htm , laddove la Commissione afferma "*In the aftermath of the terrorist attacks in Madrid in 2004 and London in 2005, the Data Retention Directive was adopted to harmonize the EU efforts in the investigation and prosecution of the most serious crimes such as, in particular, organized crime and terrorism*". Proprio tale specifica finalità, tuttavia, secondo l'analisi della Corte di Giustizia, avrebbe dovuto indurre il legislatore comunitario a porre maggiore attenzione nel disciplinare una casistica per la conservazione e l'esame di dati di traffico.

accertamenti). Anche in questo caso, rileva la Corte, non basta che la Direttiva rimandi alla legislazione di dettaglio dei singoli stati membri: è necessario che il legislatore UE fissi degli specifici criteri di base, onde garantire piena integrità e riservatezza ai dati trattati;

- in egual modo, la Direttiva non impone ai fornitori dei servizi di comunicazione elettronica dei livelli elevati di protezione e sicurezza dei dati di traffico da conservare, autorizzandoli anzi a valutare tali aspetti in relazione a considerazioni economiche, e nemmeno garantisce che, al termine del periodo di conservazione dei dati, essi vengano distrutti in maniera irreversibile;
- infine, per la Corte è grave l'assenza, nella Direttiva, di un preciso obbligo, per i fornitori dei servizi di comunicazione elettronica, di conservare e trattare i dati nel territorio dell'Unione, consentendo così agli stessi fornitori di trasferire all'estero tali attività, potenzialmente eludendo il controllo dell'Autorità indipendente competente per territorio[19].

Per le motivazioni così riassunte, la Corte di giustizia ha ritenuto che il legislatore dell'UE abbia ecceduto i limiti imposti dal principio di proporzionalità, di cui agli articoli 7, 8 e 52 della Carta dei Diritti UE, ed ha pertanto dichiarato invalida la Direttiva 2006/24/CE.

4. Effetti della sentenza comunitaria sulle normative interna ed Europea

Prima di procedere ad analizzare quali siano stati gli effetti materiali della pronuncia sopra riportata sulla normativa dei singoli Stati Membri, è utile precisare che, nelle proprie conclusioni, l'Avvocato Generale nelle cause riunite C-239/12 e C-594/12, Cruz Villalòn, pur insistendo per la invalidità della Direttiva impugnata per le motivazioni esposte al precedente paragrafo, paventava i possibili effetti della dichiarazione di nullità sulla normativa dei singoli Stati Membri e, in generale, sulle attività di prevenzione dei reati collegate alla *data retention*, soprattutto in considerazione del fatto che gli Stati Membri stessi hanno sinora fatto moderato uso delle loro competenze, per quanto riguarda le prescrizioni sulla durata massima del periodo di conservazione dei dati. Per tali ragioni, l'Avvocato Generale concludeva che, in un'ottica di ponderazione dei diversi interessi presenti nel caso in esame, sarebbe stato opportuno "*sospendere gli effetti della constatazione dell'invalidità della direttiva per dar tempo al legislatore dell'Unione di adottare le misure necessarie per porre rimedio all'invalidità accertata, restando inteso che tali misure devono essere adottate entro un lasso di tempo ragionevole*".
La Corte Europea, tuttavia, non ha ritenuto di accogliere tale conclusione, ed ha proseguito

[19] Un utile strumento per la comprensione dei princìpi in materia di Privacy applicati alla CGUE e codificati anche a livello nazionale può essere reperito in G.Finocchiaro "*Privacy e protezione dei dati personali – disciplina e strumenti operativi*", Zanichelli, 2012, p. 110 e ss.

per la dichiarazione di invalidità *sic et simpliciter* della Direttiva.
Invero, ai sensi dell'art. 267 del Trattato sul Funzionamento dell'Unione Europea, la competenza della Corte, in materia di c.d. rinvii pregiudiziali, sembra avere *efficacia diretta solo sugli atti comunitari, ma non su quelli nazionali*[20]. A ciò deve essere aggiunta la considerazione che l'art. 15 della Direttiva 2002/58/EU (tuttora valida e vigente) prevedeva la facoltà per gli Stati Membri di trasporre i principi della stessa in normativa nazionale, unitamente alle disposizioni di dettaglio che si fossero rese necessarie per la conservazione dei dati di traffico per finalità di giustizia.
Non sembra, dunque, verificarsi il vuoto normativo paventato dall'Avvocato Generale Villalòn, ma emergono, al contrario due principali effetti:
- il primo, e più immediato, è quello della "*riespansione*" dei principi generali di cui alla Direttiva 2002/58/EU: la Direttiva annullata, infatti, non abrogava né modificava alcuna previsione della previgente Direttiva;
- il secondo, e non meno importante effetto è quello della sostanziale intangibilità dei principi della Direttiva annullata già codificati in specifica normativa nazionale, da parte dei singoli Stati Membri, se non a specifiche condizioni.
Dalle previsioni sopra esaminate consegue, infatti, che gli Stati Membri che si sono limitati, a seguito delle Direttive del 2002 e del 2006, alla mera attuazione dei principi delle stesse, possono comunque, in attesa dell'approvazione di una nuova Direttiva in materia di *data retention*, dotarsi di propria normativa sulla conservazione dei dati di traffico per finalità di giustizia (ovviamente a condizione di rispettare i principi generali di cui alla sola Direttiva 2002/58/EU); nessun problema, invece, sembra sorgere, nell'immediato periodo, per gli Stati Membri (trai quali l'Italia) che hanno provveduto a trasporre i principi della direttiva in specifici atti normativi interni, dunque non sono suscettibili di effetti diretti da parte della sentenza in commento[21].

---

[20] A mente dell'art. 267 TFUE, infatti:
"*La Corte di giustizia dell'Unione europea è competente a pronunciarsi, in via pregiudiziale:*
a) sull'interpretazione dei trattati;
b) sulla validità e l'interpretazione degli atti compiuti dalle istituzioni, dagli organi o dagli organismi dell'Unione.
Quando una questione del genere è sollevata dinanzi ad un organo giurisdizionale di uno degli Stati membri, tale organo giurisdizionale può, qualora reputi necessaria per emanare la sua sentenza una decisione su questo punto, domandare alla Corte di pronunciarsi sulla questione.
Quando una questione del genere è sollevata in un giudizio pendente davanti a un organo giurisdizionale nazionale, avverso le cui decisioni non possa proporsi un ricorso giurisdizionale di diritto interno, tale organo giurisdizionale è tenuto a rivolgersi alla Corte.
Quando una questione del genere è sollevata in un giudizio pendente davanti a un organo giurisdizionale nazionale e riguardante una persona in stato di detenzione, la Corte statuisce il più rapidamente possibile."

[21] Questa ricostruzione sembra confortata anche dal disposto dell'art. 6, comma 1, del Decreto Legge n.144/2005 (c.d. "Decreto Pisanu", recante *Misure urgenti per il contrasto del terrorismo internazionale*), che già nel 2005 stabiliva che "*l'applicazione delle disposizioni di legge, di regolamento o dell'autorità amministrativa che prescrivono o consentono la cancellazione dei dati del traffico telefonico o telematico, anche se non soggetti a fatturazione, e gli stessi, esclusi comunque i contenuti delle comunicazioni e limitatamente alle informazioni che consentono la tracciabilità degli accessi, non-*

Si deve infine dare conto, pur in via residuale, di un ulteriore effetto che potrebbe verificarsi, a seguito della sentenza in commento: ferma restando la non diretta efficacia della pronuncia sulla normativa di uno Stato Membro, è comunque possibile che cittadini ed imprese di un singolo Stato Membro, presentino questione di costituzionalità della normativa privacy interna che faccia applicazione dei princìpi della abrogata Direttiva 2006/24/UE, oppure che tali soggetti propongano ricorso diretto alla Corte di Giustizia UE medesima, per l'annullamento dell'atto interno per "*violazione dei diritti fondamentali dell'UE*" (ai sensi dell'art. 263 del Trattato sul Funzionamento dell'Unione Europea[22][23]). A sommesso avviso di chi scrive, tuttavia, l'articolata motivazione resa dalla Corte a sostegno della propria decisione e la permanenza in vigore dei principi generali della Direttiva 2002/58/EU rendono poco probabile la concreta riuscita di simili mezzi di impugnativa.

5. Conclusioni

In attesa dell'intervento normativo Europeo, che con ogni probabilità riproporrà la maggior parte delle misure già disciplinate dalla Direttiva 2006/24/CE, puntando a correggerne le motivazioni e, in taluni specifici casi, la portata di dettaglio, non si può che concludere la disamina compiuta rilevando come, a livello pratico, all'esito della pronuncia in commento, la gestione dei dati personali nel settore delle comunicazioni elettroniche sia rimasta sostanzialmente immutata, in Italia come negli altri Stati Membri. In difetto di specifiche contestazioni di dettaglio, sia a livello nazionale che comunitario,

ché, qualora disponibili, dei servizi" avrebbe dovuto essere sospesa fino all'attuazione della Direttiva 2006/24/CE del Parlamento Europeo e del Consiglio e, comunque, avrebbe potuto essere proseguita "*non oltre il 31 dicembre 2008*".

[22] L'art. 263 TFUE prevede infatti che "*La Corte di giustizia dell'Unione europea esercita un controllo di legittimità sugli atti legislativi, sugli atti del Consiglio, della Commissione e della Banca centrale europea che non siano raccomandazioni o pareri, nonché sugli atti del Parlamento europeo e del Consiglio europeo destinati a produrre effetti giuridici nei confronti di terzi. Esercita inoltre un controllo di legittimità sugli atti degli organi o organismi dell'Unione destinati a produrre effetti giuridici nei confronti di terzi.*
A tal fine, la Corte è competente a pronunciarsi sui ricorsi per incompetenza, violazione delle forme sostanziali, violazione dei trattati o di qualsiasi regola di diritto relativa alla loro applicazione, ovvero per sviamento di potere, proposti da uno Stato membro, dal Parlamento europeo, dal Consiglio o dalla Commissione.
La Corte è competente, alle stesse condizioni, a pronunciarsi sui ricorsi che la Corte dei conti, la Banca centrale europea ed il Comitato delle regioni propongono per salvaguardare le proprie prerogative.
Qualsiasi persona fisica o giuridica può proporre, alle condizioni previste al primo e secondo comma, un ricorso contro gli atti adottati nei suoi confronti o che la riguardano direttamente e individualmente, e contro gli atti regolamentari che la riguardano direttamente e che non comportano alcuna misura d'esecuzione.[…]"

[23] In tema di rapporti tra diritto nazionale, diritto comunitario ed articoli 263 e 267 TFUE, si veda anche, *ex multiplis*, R.Conti "*Osservatorio della Corte di Giustizia UE – Esame della conformità di una legge nazionale con il diritto dell'Unione*", in *Il Corriere Giuridico*, n.12/2014, p.1571 e ss.

che coinvolgano direttamente la normativa dei singoli Stati Membri, infatti, essi stanno conservando i propri atti interni di attuazione della Direttiva annullata, preservando dunque il regime preesistente, in attesa di attuare una nuova versione della Direttiva sulla *data retention*.

PARTE TERZA

Contributi sul *Risk management*

N. 3 - 2015 • pp. 98-104

La Valutazione del Rischio per i Beni culturali nelle aree archeologiche

Giovanni Di Trapani e **Anna Esposito**

Abstract: Negli ultimi vent'anni si è assistito ad un profondo mutamento delle professioni collegate all'archeologia; un mutamento delle professionalità che è diventata sempre più palese nei tempi più recenti con l'istituzione di nuove procedure per la Valutazione di Impatto Archeologico.

C'è da evidenziare, però, che il quadro normativo di riferimento sebbene sia allo stato in una fase ancora embrionale,, appare chiaro, ad oggi, l'emergere di un rapporto sempre più stretto tra la professioni legate ai beni archeologici e l'attività di pianificazione territoriale, in tale contesto le problematiche legate alla gestione e valutazione del rischio archeologico assumono un ruolo di primo piano.

Parole Chiave: Risk Management, Rischio Archeologico, Beni Culturali.

1. Introduzione

Con il termine "Rischio archeologico"[1] - largamente discusso e condiviso in letteratura - s'intende un concetto articolato la cui definizione ruota attorno a due elementi fondamentali:

- il depauperamento del patrimonio storico-archeologico ovvero il "rischio per il patrimonio archeologico" di essere danneggiato in occasione di interventi di trasformazione del paesaggio;
- l'aumento dei costi di realizzazione delle opere, che si riferisce al "rischio per progettisti ed imprese" di veder compromesso il "ruolino di marcia" del progetto originale da rinvenimenti archeologici inattesi.

Il rischio archeologico è espresso, quindi, in funzione della vulnerabilità (predisposizione del bene a subire un danno in caso di evento calamitoso), della pericolosità (probabilità che si verifichi un fenomeno potenzialmente distruttivo) e dell'esposizione o valore

[1] Master in Archeologia Preventiva e Management del Rischio Archeologico - Luiss Business School Divisione di Luiss Guido Carli.

Articolo pervenuto il 10 ottobre 2015, approvato il 20 ottobre 2015

esposto (insieme dei beni a rischio presenti nell'area esposta all'evento).
Di recente, anche in relazione agli sviluppi dell'archeologia preventiva, la locuzione ha assunto un'accezione alternativa, connessa alla probabilità più o meno elevata d'intercettazione di livelli archeologici nel corso di scavi intrapresi per interventi edilizi o infrastrutturali per i quali la stratificazione archeologica rappresenta un elemento di criticità, in quanto interferisce sull'attuazione dei lavori[2].
Il mercato, si è fortemente evoluto negli anni più recenti, richiedendo figure professionali altamente specializzate, con specifiche capacità di adattamento e versatilità anche in relazione alle competenze inerenti le tecnologie più moderne. Professionalità in grado di confrontarsi con gli altri professionisti del settore (architetti, ingegneri, geometri, geologi, etc.) e nel contempo capaci di una forte approccio "problem solving"[3], in grado quindi di suggerire soluzioni tecniche concrete sia nella delicata fase della progettazione che in quella esecutiva.

2. Il Rischio Archeologico

In relazione ai recenti sviluppi della c.d. Archeologia preventiva[4], il termine Rischio Archeologico ha assunto accezioni sempre più complesse. Per R.A. si può intendere la probabilità più o meno elevata d'intercettazione di livelli archeologici nel corso di scavi intrapresi per interventi edilizi o infrastrutturali per i quali la stratificazione archeologica rappresenta un elemento di criticità.
Il Codice dei Beni Culturali e del Paesaggio, in stretta connessione con la tematica della conservazione dei beni, e precisamente all'art. 29 comma 1 e 2 sancisce che la conservazione del patrimonio culturale venga assicurata mediante una coerente, coordinata e programmata attività di studio, prevenzione, manutenzione e restauro, intendendo per prevenzione «il complesso delle attività idonee a limitare le situazioni di rischio connesse al bene culturale nel suo contesto»[5].
Allo scopo di offrire una risposta al problema del degrado del patrimonio culturale, si è avviato a partire dalla metà degli anni 90 la redazione di una Carta del rischio. Un progetto ambizioso che includeva la realizzazione di una vera e propria mappa conoscitiva dei maggiori fattori di rischio, riguardanti:

- l'aggressività dei fenomeni ambientali;
- la pericolosità antropica.

L'organo preposto al monitoraggio del Rischio Archeologico, tramite un accurato Sistema

---

[2] Enciclopedia Italiana G.Treccani.

[3] Il complesso delle tecniche e delle metodologie necessarie all'analisi di una situazione problematica allo scopo di individuare e mettere in atto la soluzione migliore.

[4] Settore della ricerca archeologica che concilia la tutela del patrimonio con le esigenze operative di interventi edilizi, estrattivi o relativi a grandi opere infrastrutturali, che comportano lavori di scavo.

[5] Decreto Legislativo 22 gennaio 2004, n. 42 "Codice dei beni culturali e del paesaggio".

Informativo Territoriale è l'Istituto centrale per il restauro[6] istituito, ai sensi dell'articolo 8 del decreto legislativo 20 ottobre 1998, n. 368 e successive modificazioni. La realizzazione della Carta del Rischio consiste, come detto, in un vero e proprio sistema informativo territoriale inteso a determinare non solo la gravità, ma anche l'urgenza del rischio, ed è composto da un più che articolato sistema di banche dati alfanumeriche e cartografiche in grado di valutare, attraverso un approccio statistico, il livello di vulnerabilità e quindi di rischio dei beni (archeologici, monumentali, ecc).
Mediante l'applicazione di analisi statistiche, sulla base di un'azione di tipo conoscitivo volto all'individuazione della vulnerabilità e al rischio in senso stretto si è giunti ad una previsione del Rischio Archeologico individuando per territorio i livelli di probabilità di presenza archeologica. L'approccio scientifico dalle potenzialità evidentemente predittive ha consentito, superando la iniziale nozione di Carta del Rischio, l'elaborazione di un Sistema che amplifica ed evolve in un nuovo modello di carta del potenziale archeologico.

Figura 1 Carta del Rischio del Patrimonio Culturale – I.C.R.

Fonte: www.cartadelrischio.it

[6] Istituito con DM del 7 ottobre 2008, è organo tecnico del *Ministero dei beni e delle attività culturali e del turism.*

2.1 I fattori di Rischio

Per la costruzione del modello di rischio, l' Istituto centrale per il restauro ha adottato, sulla base dei singoli beni, un approccio strettamente statistico che mira all'individuazione ed alla valutazione dei livelli di rischio. I fattori di Rischio individuati possono essere suddivisi in due macro categorie:

- la Vulnerabilità Individuale;
- la Pericolosità Territoriale.

La prima, indica l'esposizione di un dato bene all'esposizione di fattori territoriali ed ambientali, la seconda fa riferimento al livello di potenziale aggressività di una data area territoriale.
Il modello elaborato, quindi, qualifica le due componenti e ne valuta l'intensità attraverso la misura delle grandezze fisiche individuando tre differenti *domini* validi sia per i fattori di rischio legati alla Vulnerabilità che a quello della Pericolosità Territoriale. Tali domini sono stati codificati in:

- Ambientale-Aria;
- Statico-Strutturale;
- Antropico.

Per quanto concerne, allora i fattori di Vulnerabilità si riferiscono all'aspetto della superficie, alle caratteristiche costruttive e statico-strutturali ed, infine, all'uso e alla sicurezza. Viceversa, per i fattori legati alla Pericolosità Territoriale i domini sono caratterizzati dai fattori climatici, microclimatici e gli inquinanti dell'aria, dalle caratteristiche geomorfologiche del suolo e del sottosuolo, dalle dinamiche demografiche e socioeconomiche.
Il modello elaborato esprime il Rischio come funzione proprio delle due componenti Vulnerabilità (V) e Pericolosità (P) e sarà così espresso:

Equazione 1 - Il Modello Logico del Sistema Informativo Territoriale della Carta del Rischio.

$$R = R(V1, V2, \ldots Vn, P1, P2, \ldots Pn)$$

dove R denota l'Indicatore di Rischio e si configura come una media ponderata degli Indicatori di Vulnerabilità (V) e di Pericolosità (P).

Fonte: www.cartadelrischio.it

3. La valutazione dell'impatto archeologico

L'individuazione delle fonti per un inquadramento normativo della valutazione dell' impatto archeologico trova fondamento nella direttive europe 2001/42/CE sulla Valutazione Ambientale Strategica, 85/337/CEE sulla Valutazione di Impatto Ambientale e 92/43/CEE sulla Valutazione di Incidenza Ambientale.

Un articolato normativo complesso che prevede, dunque, la compresenza di ben tre procedure valutative; in estrema sintesi, gli approcci nell'applicazione delle differenti procedure considerano:

- tre corpi valutativi come atti autonomi e separati;
- l'integrazione metodologica e procedurale in coerenza con i principi di analisi e valutazione ambientale.

Una modalità che si può evidentemente realizzare solo attraverso un approccio di tipo interdisciplinare[7] tra saperi: geologiche, naturaliste, archeologiche, etc.
Fondamentale a tal proposito sarà l'elaborazione di tecniche quali-quantitative capaci di definire il "valore" delle diverse componenti ambientali costituenti un determinato ambito geografico in cui s'intende realizzare una trasformazione territoriale[8]. Ai fini strettamente valutativi nella pianificazione territoriale sono tre i Sistemi che rivestono un ruolo determinante, e precisamente quello:

- biotico;
- abiotico;
- umano.

Il primo si riferisce alla flora e alla fauna, il secondo alla struttura geologica, idrogeologica, ed alla struttura fisico-chimica delle acque. Infine, il terzo afferisce la struttura sociale, economica e culturale. Dal punto di vista metodologico il "valore", che può essere denominato con il termine di sensibilità (S), di una componente è frutto del prodotto tra la fragilità (f), intrinseca nella componente, e la sua vulnerabilità (v).

Equazione 2 - Il "valore" di una componente ambientale

$$S = f * v$$

Fonte: Metodologia per la valutazione dell'impatto archeologico - Archeologia e Calcolatori n. 18/2007, Campeol G., Pizzinato C.

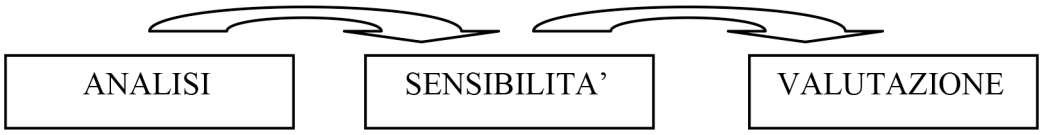
La Fragilità è intesa come la caratteristica propria di una componente e la Vulnerabilità come la probabilità che detta componente possa essere "colpita" da una fonte di pressione esterna.
Dall'analisi dell'evoluzione normativa è facilmente intuibile che il legislatore ha avuto in intenzione con provvedimenti successivi di cercare limitare gli impatti sulla struttura biotica, abiotica ed umana dell'ambiente, producendo danni non solo alla qualità dell'acqua dell'aria o del patrimonio archeologico ma generano danni per lo più economici.
Nel merito si può affermare che la Valutazione dell'impatto ambientale introdotto con le successive normative vigenti abbia un peso per lo più di carattere preventivo. Infatti, i procedimenti prevedono, attraverso stime e simulazioni, l'individuazione delle possibili modificazioni future provocate anche in modo involontario su un territorio o area

[7] McHarg 1989 e Steiner 1994.

[8] Campeol G., Pizzinato C. 2007

geografica. Appare ovvio che,alla luce di quanto evidenziato, la valutazione dell'impatto ambientale abbia un alto valore di sostegno alla realizzazione progettuale traducendosi quindi in un procedimento "interno" alla redazione di un progetto.
D'altro canto, la componente archeologica, si ritiene, vada intesa "come parte del sistema ambientale e non come oggetto valutativo"; ne consegue che nella fase di individuazione del Rischio le fasi di valutazione tendano a misurare con metodo probabilistico il mero impatto negativo sulla presenza di oggetti e manufatti di interesse archeologico

Figura 2 Le fasi della Valutazione dell'impatto archeologico.



Fonte: ns Elaborazione

La valutazione dell'impatto archeologico si sviluppa generalmente lungo tre direttrici: una prima di *Analisi, una seconda di studio della Sensibilità*[9] - in cui si individuano le origini storiche e possibili trasformazioni geomorfologiche e ambientali del territorio - *ed infine, nella definizione vera e propria del livello di Rischio.*

4. Conclusioni

La Valutazione del Rischio e la successiva elaborazione di una documentazione sistemica di una Carta del Rischio ha come scopo iniziale l'individuazione di alcune caratteristiche delle strutture archeologiche ritrovate. Tali caratteristiche afferiscono a:

- Collocazione;
- Profondità;
- Ingombro.

Tale procedura non può, però, esaurirsi in un mera accatastamento dei ritrovamenti archeologici ma deve tendere soprattutto a valutazioni ed elaborazioni previsionali dei comportamenti umani - volontari ed involontari – sulle strutture esistenti. Come evidenziato nel corso del lavoro, le fasi di elaborazione e valutazioni seguono logiche fondate su logiche di prevedibilità con approccio quali-quantitativo e statistico dell'impatto ambientale ed archeologico.
Le fasi del procedimento di registrazione e successive segnalazioni archeologiche rappresentano un valido strumento preventivo alle fasi di programmazione territoriale.

[9] "Per sensibilità si intende il valore di unicità che viene conferito all'oggetto appartenente ad un determinato periodo storico, utilizzando come parametri l'antichità, la rarità e il livello di conservazione, nonché il pregio artistico." Fonte Campeol G., Pizzinato C. 2007

Ne consegue che il rapporto non sempre lineare che contraddistingue l'archeologia ed il mondo esterno pone problematiche nuove, tema questo che impatta sulle scelte anche di carattere di pianificazione del territorio, e che arricchiscono il più che dibattuto argomento della tutela, della conservazione nonché della valorizzazione dei Beni culturali ed archeologici.

Bibliografia

- CAMPEOL G., PIZZINATO C. (2007), Metodologia per la valutazione dell'impatto archeologico Archeologia e Calcolatori 18, pp 273-292;
- COVIELLO A., (2004) Risk Management, Confapi Caserta, Collana Centro Studi e Ricerche;
- COVIELLO A. (2005) Il governo dei rischi d'impresa, G. Giappichelli Editore;
- DI TRAPANI G. (2013) Profili E Principali Approcci Alle Coperture Dei Rischi Catastrofali, in A. Coviello, CALAMITA' NATURALI E CPOPERURE ASSICURATIVE Il Risk Management nel Governo dei Rischi Catastrofali Dario Flaccovio Editore Coll. SIGEA di Geologia Ambientale ISBN 978-88-579-0209-8;
- DI TRAPANI G. (2013), Rischi nella Valorizzazione delle aree archeologiche nell'ambito del Convegno Valorizzazione del patrimonio sommerso di Sinuessa Civico curato dal Comune di Sessa Aurunca e dall'ENEA in Sessa Aurunca (CE)Piazza Castello - 30 Aprile 2013
- DECRETO LEGISLATIVO 22 gennaio 2004, n. 42 "Codice dei beni culturali e del paesaggio";
- MCHARG J. (1989), Progettare con la natura, Padova, Muzzio;
- MINOPOLI C., PICA R., TROCCIOLA A., DI TRAPANI G, 2012-Valorizzazione dell'area archeologica marina di Sinuessa (Sessa Aurunca - CE), 2° Workshop Erosione costiera in siti di interesse archeologico, d'Italia e la Marina Militare, Napoli, 5 Ottobre 2012;
- STEINER F. (1994), Costruire il paesaggio, Milano, McGraw-Hill Editore;
- TROCCIOLA A., PICA R, SARAO P., MINOPOLI C., RUGGI D'ARAGONA M.G., DI TRAPANI G. (2012) Elementi per lo sviluppo sostenibile dell'Area Martina Protetta di Sessa Aurunca CATALOGO Attività 2012 ENEA

N. 3 - 2015 • pp. 105-??

Il Risk Management nelle imprese italiane tra prevenzione e ritenzione dei rischi.

Antonio Coviello e **Giovanni Di Trapani**

Abstract: La scarsa attenzione nei confronti del governo dei rischi d'impresa appare sinora addebitabile alla tendenza dei manager italiani a sottovalutare o ad ignorare i rischi di evento dannoso e all'incapacità di sviluppare quell'atteggiamento orientato alla sicurezza, che trova più frequentemente riscontro in altri paesi sviluppati. Il rischio è alla base delle decisioni strategiche ed, allora, valutare il rischio globale dell'impresa è un'operazione sicuramente difficile e costituisce per l'organo di governo dell'impresa l'elemento qualificante ed, in ultima istanza, determinante per garantire un'evoluzione risonante dei rapporti sistemici. Il presente lavoro intende valutare le diverse modalità per governare i rischi d'impresa, attraverso le sue molteplici opzioni, fra politiche di prevenzione e di protezione, oltre alla capacità di saper intercettare le opportunità offerte dai mercati assicurativi e finanziari di riferimento, in un'epoca in cui assume sempre più importanza la attenta valutazione dei rischi di natura "etica."

Parole Chiave: Risk Management, Innovazione e Servizi per lo Sviluppo, *Insurance.*

Introduzione

Uno dei principi cardine del *Risk Management,* prevede la gestione secondo una logica unitaria della sicurezza fisica e dell'assicurazione.

Questi due strumenti possono trovarsi fra loro in rapporto di complementarietà o di sostituibilità. Mentre i rapporti di complementarietà fra prevenzione ed assicurazione sono abbastanza banali - a condizione che la compagnia analizzi seriamente la qualità del rischio assunto e calibri di conseguenza i premi praticati - è indubbio che esista sempre una lucida comprensione dei rapporti di sostituibilità.[1]

La ritenzione del rischio è una soluzione praticabile quando il rischio, o certe quote di rischio, siano sopportabili con le normali risorse finanziarie aziendali. È noto che, se consideriamo i flussi finanziari positivi e negativi che ne derivano, l'assicurazione non

[1] Cfr. Carniol F. , *Risk Management. Strumenti e politiche per la gestione dei rischi puri d'impresa*, Cerap, Egea, Milano, 1996.

Articolo pervenuto il 10 ottobre 2015, approvato il 20 ottobre 2015

è mai economicamente conveniente nel lungo periodo. Infatti, se il premio pagato dal cliente è maggiore, salvo errate valutazioni dell'assicuratore, della perdita media attesa legata al rischio sopportato senza grave turbamento dell'equilibrio finanziario - aziendale, la ritenzione può rivelarsi una soluzione interessante e vantaggiosa.[2]
Senza voler indulgere ad una finanziarizzazione del *Risk Management,* è indubbio che la ritenzione rappresenti, rispetto alla prevenzione e all'assicurazione, un terzo polo di interesse cui la gestione dei rischi puri deve dedicare molta attenzione. Un *Risk Management* evoluto e moderno implica, dunque, che il *risk manager* dedichi parte della sua attività alla pianificazione finanziaria degli interventi, da realizzare in stretta collaborazione con la Direzione Finanza.

1. Le metodologie di decisione.

Le metodologie decisionali sono l'insieme di approcci, tecniche, regole impiegate per scegliere, fra due o più alternative disponibili, quella più conveniente in rapporto a dati obiettivi.
Tutti i problemi ammettono come minimo due alternative, perché si deve in ogni caso decidere almeno fra il fare e il non fare nulla.
In un'impresa, le metodologie decisionali devono avere una caratterizzazione economica, dato che economica è la natura degli obiettivi da raggiungere. Ciò significa che, in linea di principio, la risoluzione di qualsiasi problema decisionale deve essere individuata mediante un raffronto dei costi e dei ricavi associati alle alternative a disposizione. Si sottraggono a questa logica i casi in cui un comportamento è obbligatorio, oppure, giustificato da considerazioni strategiche che sfuggono alla quantificazione economica.
Nel campo del *Risk Management,* le metodologie decisionali soffrono dell'elevata incertezza dei rischi puri. Per decidere in maniera economicamente corretta, si dovrebbe conoscere con esattezza la perdita che un certo rischio arrecherà in un dato periodo, ma, evidentemente, questa informazione si potrebbe acquisire solo se il rischio fosse certo ossia se il rischio non fosse rischio.
Ne consegue che è inevitabile dare spazio nel *Risk Management* a metodi di decisione meno rigorosi, in cui giochino esperienza personale e regole empiriche. Ciò senza comunque escludere il calcolo economico, che può essere esercitato anche su informazioni incerte, purché dotate di buona credibilità, a condizione di realizzare un serio lavoro di identificazione e valutazione, così da ottenere informazioni valide su molti rischi, soprattutto su quelli di non rarissima manifestazione.[3]

---

[2] Così Forestieri G., *Risk Management: strumenti e politiche per la gestione dei rischi puri dell'impresa*, op.cit.

[3] Space- centro europeo per gli studi sulla protezione aziendale, *Indagine generale sul Risk Management*, 1994

Il *broker* e l'*assicuratore* sono un importante parametro di riferimento nelle decisioni[4]; a volte poi vi è un atteggiamento di accettazione passiva delle disposizioni di legge, o a seconda dei casi, dell'opinione del broker o dell'assicuratore. In imprese altamente decentrate e contraddistinte da scale gerarchiche allungate, il vertice interviene direttamente solo su materie rilevanti e pertanto il suo coinvolgimento nel *Risk Management* deve essere interpretato come un segnale di interesse verso le problematiche dei rischi puri. Al contrario, nelle imprese accentrate e gerarchicamente corte, il vertice, che spesso coincide con la proprietà, tende a partecipare a qualunque decisione e la non rara assunzione diretta della gestione dei rischi puri, intesa quale mero acquisto di polizze assicurative, deve essere vista come indicatore di una sostanziale inesistenza di *Risk Management*.[5]

2. Il ruolo del risk manager tra strategia e prevenzione.

Il *risk manager* affonda le sue radici nella figura dell'*insurance manager,* cioè del responsabile assicurativo che, a seguito dello sviluppo del processo di gestione del rischio, ha visto ampliare ed approfondire progressivamente i propri compiti. Il *risk manager* non è, quindi, mero gestore di polizze o di relazioni con il mondo assicurativo, ma figura complessa alla quale è demandata la gestione, in senso lato, dei rischi puri dell'impresa, ed in particolare sia dei rischi assicurabili che di quelli non assicurabili.[6]
La presenza del *risk manager* consente di decidere l'acquisto del prodotto assicurativo eventualmente avvalendosi della consulenza di un tecnico esterno (quale *broker* o altra figura) ma, in ogni caso, evitando di esternalizzare il processo decisionale, cosicché, la valutazione delle alternative avviene nell'esclusivo interesse dell'azienda e anche dalle imprese assicuratrici, in grado di erogare un servizio assicurativo di qualità, tagliato su misura per rispondere alle reali esigenze - necessità del cliente/utilizzatore, le quali, evidentemente potranno beneficiare del lavoro svolto dal *risk manager.*[7] "L'uomo che è denominato *risk manager* è qualcosa di più di un consulente sul trattamento del rischio o forse, meglio ancora, di un coordinatore di questo trattamento. Il suo lavoro è interdisciplinare, è quello dell'ufficiale di collegamento. Deve sviluppare un collegamento con le altre funzioni dell'azienda, come direttori di impianti, tecnici di officina, ingegneri, progettisti, uffici acquisti, direttori della distribuzione, delle spedizioni, dell'imballaggio, delle vendite e così via, per rendere chiaro a tutti che il trattamento del rischio è

---

[4] Cfr. Coviello A.-Pellicano M., *La gestione del marketing nelle imprese assicuratrici* – Cedam, Padova, 1999

[5] Tagliavini P. - Misani N., *Indagine generale sul risk management in Italia*., 1999, op. cit..

[6] 19 Forestieri G., *Il risk management: strumenti e politiche per la gestione dei rischi puri dell'impresa*, Cerap, Egea, Milano, 1996

[7] Cfr. Coviello A., *Così il risk manager aiuta l'impresa* - Il Denaro n.41, 1998

responsabilità di tutti. Il lavoro del *risk manager* può soltanto essere di assistenza alla direzione nella identificazione dei rischi e ciò è possibile fare abitualmente con questioni di senso comune di profani. Dopo aver identificato il problema è necessario ottenere il sostegno e l'assistenza delle altre funzioni per trovare una risposta ad esso. Con il passare del tempo, si svilupperà in tutta l'azienda un atteggiamento mentale, cosicché tutte le funzioni si identificano nei rischi e di conseguenza nella loro valutazione e nel loro controllo".[8]

Si ritiene tuttavia che il *risk manager* non abbia ad essere un esperto delle diverse funzioni in cui si articola il sistema aziendale, in modo da poterne cogliere personalmente tutti i possibili rischi, ma debba essere più propriamente colui che da un lato sensibilizza i vari responsabili di funzione o di settore nei confronti di una ottimale gestione dei rischi fornendo gli strumenti necessari e, dall'altro, rappresenti un punto di riferimento presso il quale convergono tutte le informazioni[9] funzionali all'identificazione e qualificazione, in termini di frequenza e gravità del rischio.

Lo svolgimento di queste due fasi preliminari, nelle quali il *risk manager* deve essere coadiuvato dai vari responsabili, culmina con la fase di determinazione delle differenti metodologie di trattamento degli specifici rischi e nel compito del *risk manager* di coinvolgere attivamente i vari responsabili nell'attuazione delle strategie proposte. Quindi il *risk manager* dovrebbe essere considerato un coordinatore delle diverse funzioni aziendali nell'ottica di un ottimale gestione del rischio.

La particolare attività svolta, la stretta collaborazione con i vertici delle varie aree, la possibilità di invadere talvolta le competenze altrui (con un'ampia autonomia decisionale), suggeriscono di collocare questa figura nelle posizioni di vertice dell'organigramma aziendale, facendogli acquisire in tal modo la necessaria autorevolezza per dare maggiore incisività alle proprie azioni.[10]

Nella realtà italiana la figura del *risk manager,* nella sua forma più evoluta, risulta rara e presente solamente nelle imprese di grandi dimensioni, anche se negli ultimi anni il livello dimensionale minimo per rendere economicamente conveniente il suo impiego, tende a diminuire. La difficoltà di diffusione di tale figura, pare imputabile - tra l'altro - ad una sensibilità non sufficientemente sviluppata verso la gestione del rischio (da parte del *top management* e del mondo assicurativo), oltre alla difficoltà di riuscire a valutare la sua portata e quella dell'intero processo di *risk management* in termini di analisi costi - benefici.[11]

---

[8] Così Bannister & Bawcutt, *Manuale di risk management*, Golden Book, 1981

[9] Ci si riferisce alle informazioni provenienti dai vari settori o dalle varie funzioni d'impresa.

[10] Cfr. Paci S., *Risk management strumenti e politiche per la gestione dei rischi puri dell'impresa*, a cura di G. Forestieri, Cerap, Egea, Milano, 1996

[11] Per maggiori approfondimenti si veda Forestieri G., *Risk management: strumenti e politiche per la gestione dei rischi puri dell'impresa*, Cerap, Egea, Milano, 1996, op. cit.

3. Gli strumenti a disposizione del risk manager

Dopo aver analizzato il ruolo ed i compiti del *risk manager,* appare necessario descriverne le mansioni (*job description*).
Si è già accennato all'importanza della personalità, aiutata da una conveniente posizione nell'azienda e dal sostegno del top management; in aggiunta a tale caratteristica, il *risk manager* deve essere desideroso di apprendere e mostrare una forte inclinazione a indagare su tutti gli aspetti delle attività dell'azienda che possano implicare minacce all'attività stessa. Il *risk manager* deve essere dotato di immaginazione, deve essere portato al contatto umano, con l'abilità di stabilire con ciascuno il rapporto giusto.[12]
Si dice che il *risk manager* debba essere prima di tutto un profondo conoscitore di uomini, oltre che della tecnologia incorporata nella funzione di produzione, della tipologia dei fattori utilizzati e della qualità degli *output.*
Entrano allora in gioco le doti personali, con le quali sviluppare e mantenere i contatti umani, spingere e realizzare il lavoro di èquipe.[13]
Il *risk manager* ideale dovrebbe, inoltre, possedere un atteggiamento equilibrato verso il rischio. Dovrebbe saper affrontare il rischio senza essere incauto, non dovrebbe cioè essere contrario al rischio nel senso di cercare la sicurezza ad ogni costo. Questo atteggiamento equilibrato dovrebbe avere il sostegno della conoscenza delle tecniche della contabilità, di una profonda comprensione di tutti gli aspetti dell'attività dell'azienda, sia commerciali che di produzione, di una buona esperienza nel campo assicurativo e del controllo perdite, nella protezione contro gli incendi ed altri pericoli materiali. Deve avere, inoltre, delle cognizioni sui comportamenti delle persone e sui modi in cui questi comportamenti possono tradursi in rischi.[14] Qualunque sia l'obiettivo che il *risk management* d'impresa si propone di perseguire, la sopravvivenza dell'azienda nel lungo periodo dipende dal livello di profitti e dal grado di soddisfazione degli azionisti che ne deriva. È per questo che gli organi esecutivi dell'impresa devono essere ben consapevoli di come le politiche da loro perseguite influenzano il prezzo delle azioni.[15]
Il *risk manager*, dal canto suo, deve prendere le proprie decisioni avendo ben presenti le prospettive di cambiamento dell'azienda e dell'ambiente nel quale essa opera, nonché dei vincoli che ne derivano.[16]
Gli strumenti a disposizione del *risk manager* per la gestione dell'incertezza sono raggruppabili in due classi: il *controllo fisico* ed il *controllo finanziario* delle perdite. Anche se molte considerazioni di tipo non economico potrebbero influenzare il processo di decisione relativo al controllo fisico delle perdite, in ultima analisi ci sono dei limiti

---

[12] Bannister & Bawcutt, *Manuale di risk management*, Golden Book, 1981

[13] Chiarlo M., *Economia dell'assicurazione danni*, Ecig, Genova, 1993

[14] Bannister & Bawcutt, *Manuale di risk management*, Golden Book, 1982

[15] Cfr. Banham R.Anderson, *Managing risk in the 21st century*, by Risk Management, April, 1994.

[16] Per un maggiore approfondimento, si consulti Barlow, *The evolution of risk manager*, by Risk Management, April, 1993.

al di là dei quali le implicazioni finanziarie non possono essere trascurate. Esistono, infatti, delle strette relazioni fra la gestione del costo del rischio da un lato e la sicurezza finanziaria, nonché gli effetti sui flussi di cassa dall'altro.
Il *risk manager* deve in particolare considerare gli effetti delle proprie strategie su:

- costo atteso del rischio;
- andamento temporale della variabilità di costi e profitti;
- variazione di breve periodo nei flussi di cassa;
- andamento della liquidità;
- tasso di redditività dell'attività aziendale al lordo delle tasse;
- trattamento fiscale delle perdite, dei prezzi di assicurazione, degli strumenti per i fondi rischi;
- disponibilità ed il costo del finanziamento esterno.[17]

Se questi fattori ora elencati, costituiscono dei vincoli più o meno stringenti per il *risk manager*, la loro intensità varia da azienda ad azienda e nel tempo. Vi sono numerosi modi per raggiungere le potenzialità di crescita di un'azienda.
È essenziale servirsi di tre parametri di particolare rilevanza: la liquidità, la profittabilità e la capacità di ottenere finanziamenti. Un livello elevato di questi indicatori esprime un buono stato di salute dell'attività e, di conseguenza, porta ad un alleggerimento dei vincoli operativi per il *risk manager.*
In questo caso sarà possibile orientare l'attività di *Risk Management* verso quelle politiche di controllo del rischio che offrono maggiori profitti in una prospettiva di medio e lungo periodo: il controllo fisico delle perdite, una elevata ritenzione del rischio e lo stanziamento di fondi, la capitalizzazione delle perdite.[18]
Un deterioramento delle condizioni richieste rende i vincoli più stringenti e obbliga il *risk manager* ad elaborare una strategia che dedichi solo uno spazio ridotto alle politiche di prevenzione e di ritenzione del rischio, per concentrarsi sulle operazioni di trasferimento.
È indubbio che lo sviluppo delle aziende del nostro tempo sembra dipendere sempre più prepotentemente da una molteplicità di condizioni e circostanze intangibili quali la qualità del *management*, il patrimonio tecnologico, la fiducia dei clienti, la cultura organizzativa, la capacità innovativa e quant'altro; tutti fenomeni che, seppur sfuggiti ad un processo di determinazione quantitativo e monetario, non possono astenersi dal rientrare in un adeguato processo di analisi dei costi, perché tale processo non riguarda soltanto il problema dell'efficienza operativa della produzione, bensì, va visto e letto, come un fenomeno più complesso, legato alle variabili competitive e sociali del sistema aziendale, agli assetti organizzativi e manageriali, allo sviluppo del patrimonio intangibile[19].
L'innovazione, la flessibilità, la dominanza, non rappresentano semplicemente il risultato di investimenti oculati di lungo termine, operati dalla direzione aziendale, in quanto la

---

[17] Così Banham R.Anderson, *Managing risk in the 21st century*, by Risk Management, April, 1994

[18] Leyents A., *Determining accettable risks levels*, by Risk Management, October, 1993.

[19] Cfr. Barlow, *The evolution of risk manager*, by Risk Management, April, 1993 e Banham R.Anderson, *Managing risk in the 21st century*, by Risk Management, April, 1994

gestione strategica non può essere costretta soltanto alla linearità dei rapporti di causa ed effetto.
Le relazioni di modalità o di funzionalità tra le leve decisionali a disposizione della direzione strategica e le risorse strutturali delle aziende, sono fenomeni in stretta correlazione tra loro e influenzano, a loro volta, il sistema organizzativo e manageriale, il comportamento dei clienti-utenti e dei concorrenti, nonché la collaborazione degli interlocutori sociali.
È importante porre in evidenza i rapporti fra obiettivi possibili e mezzi convenienti per il loro raggiungimento. Tali obiettivi, possono essere perseguiti considerando le opzioni consentite dalla tecnologia, dalle strutture operative ed organizzative in atto o potenziali; dalle risorse umane ed invisibili, disponibili o sviluppabili.
Alcuni elementi, più di altri, hanno avuto una maggiore influenza sull'introduzione del *Risk Management* in Italia. Si tratta del livello di cultura dell'imprenditore (e, di conseguenza, di quello diffuso all'interno dell'impresa); del livello di apprendimento e, infine, del livello di collaborazione e di apertura dell'impresa verso l'esterno. In particolare il *livello di cultura* presente in azienda può essere identificato in due momenti fondamentali: il ruolo e la cultura dell'imprenditore, la qualificazione e il grado di coinvolgimento della forza lavoro presente nell'impresa.
Questi due momenti appaiono quasi sempre correlati, concretizzandosi nel complesso degli atteggiamenti funzionali al successo dell'impresa, i quali si assimilano dall'imprenditore con il passare del tempo. Affinché si possa effettivamente parlare di *cultura d'impresa*, è necessario che ci sia una cultura del gruppo, per certi versi autonoma rispetto a quella dell'imprenditore, anche se certamente derivata da quest'ultima.
La *cultura organizzativa*, inoltre, risulta correlata ai processi di apprendimento, in quanto questi ultimi consentono di sottoporre a verifica una serie di ipotesi di base (relativamente alla sperimentazione di percorsi alternativi per la ricerca delle migliori soluzioni di adattamento esterno e di integrazione interna), e i risultati sono rappresentati da un patrimonio di conoscenze e di meccanismi operativi che vengono considerati validi come percorsi corretti per percepire, e gestire, i problemi che si presentano.
La cultura d'impresa sarà, dunque, il risultato di una interazione continua tra le ipotesi e le teorie che i fondatori portano inizialmente nel gruppo, ed il percorso di esperienza di quest'ultimo può atteggiarsi in misura differente a seconda della maturità culturale dell'imprenditore e del suo gruppo.
Il *livello di apprendimento,* che si sviluppa all'interno dell'impresa, dipende dall'impostazione strategica pianificata, al fine di consentire alle conoscenze individuali di trasformarsi in patrimonio collettivo[20].

[20] Si tratta di un percorso circolare, attraverso il quale si procede alla cessione - acquisizione di competenze tra persone e gruppi, finalizzato alla creazione di conoscenze capaci di facilitare l'autonomia, la collaborazione, l'approccio integrato dei problemi e, infine, ad agevolare i percorsi innovativi.

4 Conclusioni

È importante, allora, per l'imprenditoria (grande e piccola) italiana un adeguamento agli standard europei (vedi Inghilterra), e mondiali (vedi Stati Uniti d'America), dove lo sviluppo e la crescente importanza della funzione di *Risk Management*, ha avuto negli anni un'importanza sempre crescente, e un'applicazione sempre più ponderata alle esigenze delle imprese, anche di piccole dimensioni, guardando alla figura del *risk manager* come alla possibilità di trovare la giusta risposta ai fenomeni anomali che si verificano nella vita delle imprese.

Urge una approfondita riflessione sul fenomeno *Risk Management*, che possa stimolare un dibattito mirato sulla reale applicazione dello stesso alla realtà italiana, disegnando un quadro ove questo approccio si possa in vario modo inquadrare e ricondurre, comunque ai diversi comportamenti strategici assunti e agli obiettivi di politica industriale prefissati, così da auspicarsi quella crescita culturale del *management* italiano da più parti invocata, per poter dare anche una diversa configurazione agli strumenti che il mercato offre ed offrirà per la gestione del rischio.

La maggiore attenzione alla gestione dei rischi di impresa è riferita essenzialmente alle fasi di cambiamento in atto, sintetizzati come cambiamenti improvvisi, urgenti, decisi rapidamente e sollecitati, e quasi sempre, resi necessari da contesti difficili, in cui può essere in dubbio la stessa sopravvivenza dell'impresa.

Sono pur sempre cambiamenti importanti o addirittura radicali e traumatici che investono non solo le strategie ma anche la cultura ed in molti casi gli stessi assetti proprietari, coinvolgendo anche gli *stakeholders*[21] ai quali è richiesto impegno e sacrificio, il tutto in vista di un obiettivo genericamente espresso dal ritorno dell'impresa all'equilibrio, alla redditività, allo sviluppo ulteriore, cioè ad una vita normale e proiettata sul lungo termine.

[21] Occorre considerare gli stakeholder come soggetti che contribuiscono al processo di creazione del valore, e che quindi entrano a pieno titolo nel sistema di gestione strategica dell'impresa. Possiamo poi distinguere tra stakeholder interni, ossia quei soggetti che agiscono all'interno del sistema impresa (ad esempio la proprietà, la direzione e le risorse umane aziendali); gli stakeholder esterni, ossia coloro che esercitano dall'esterno un'influenza sulle vicende dell'impresa (ad esempio lo Stato, i sindacati, l'opinione pubblica); gli stakeholder primari, ossia coloro che hanno una formale relazione contrattuale con l'impresa (ad esempio i fornitori, i lavoratori, e i clienti) e gli stakeholder secondari, ossia tutti gli altri soggetti e/o gruppi influenzati in modo indiretto dall'impresa, che possono influenzare o essere influenzati dalle attività d'impresa. Così Coviello A.-Pellicano M., *Marketing assicurativo,* Liguori Editore, 2010

Bibliografia

- ADAM, A., & SHAVIT, T. 2009, Roles and responsibilities of boards of directors revisited in reconciling conflicting stakeholders interests while maintaining corporate responsibility. Journal of Management and Governance;
- ARENA, M., ARNABOLDI, M., & AZZONE, G. 2010, The organizational dynamics of enterprise risk management. Accounting, Organizations and Society;
- BORGHESI A., GAUDENZI B. – 2011, Risk management nella supply chain Sinergie rivista di studi e ricerche, 2011 - eng.sinergiejournal.it;
- BROOKS, D.W., FRASER, J., & SIMKINS, B. J. 2010, Creating a Risk-Aware Culture. Enterprise Risk Management, 87-95;
- CAS. 2003b, Overview of enterprise risk management. Paper presented at the Casualty actuarial society;
- CHECKLEY, M. 2009,. Inadvertent Systemic Risk in Financial Networks: Venture Capital and Institutional Funds. Long Range Planning, 42, 341-358;
- COVIELLO A., Di Trapani G, 2013, Supply Risk Management: Mitigation Strategy - Journal of Economic Behavior vol. 3, 2013 October 14, 2013 169-176;
- DONZA G. – 2008, Il sistema di controllo interno nella prospettiva del risk management - Giuffrè Editore (collana Studi economico-aziendali E. Giannessi;
- FLOREANI A.– 2014, La valutazione dei rischi e le decisioni di risk management - EDUCatt Università Cattolica;
- HOYT, R. E., & LIEBENBERG,A. P. 2011,The value of enterprise risk management. Journal of Risk and Insurance;
- ISO 31000. 2010. Risk Management – Principles and guidelines, from http://www.iso.org/iso/home/standards/iso31000.htm;
- NEPI A. – 2007, Project risk management: analisi e gestione dei rischi di progetto – Franco Angeli Editore;
- PRANDI P. – 2010, Il risk management. Teoria e pratica nel rispetto della normativa – Franco Angeli Editore;
- RISALITI G. – 2008, Gli strumenti finanziari derivati nell'economia delle aziende. Risk management, aspetti operativi e principi contabili internazionali – Giuffrè Editore.